FIGHTING IDENTITY THEFT—THE ROLE OF FCRA

HEARING

BEFORE THE

SUBCOMMITTEE ON
FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

JUNE 24, 2003

Printed for the use of the Committee on Financial Services

Serial No. 108–42

U.S. GOVERNMENT PRINTING OFFICE

92–902 PDF WASHINGTON : 2003

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

HOUSE COMMITTEE ON FINANCIAL SERVICES

MICHAEL G. OXLEY, Ohio, *Chairman*

JAMES A. LEACH, Iowa
DOUG BEREUTER, Nebraska
RICHARD H. BAKER, Louisiana
SPENCER BACHUS, Alabama
MICHAEL N. CASTLE, Delaware
PETER T. KING, New York
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
ROBERT W. NEY, Ohio
SUE W. KELLY, New York, *Vice Chair*
RON PAUL, Texas
PAUL E. GILLMOR, Ohio
JIM RYUN, Kansas
STEVEN C. LATOURETTE, Ohio
DONALD A. MANZULLO, Illinois
WALTER B. JONES, JR., North Carolina
DOUG OSE, California
JUDY BIGGERT, Illinois
MARK GREEN, Wisconsin
PATRICK J. TOOMEY, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
JOHN B. SHADEGG, Arizona
VITO FOSSELLA, New York
GARY G. MILLER, California
MELISSA A. HART, Pennsylvania
SHELLEY MOORE CAPITO, West Virginia
PATRICK J. TIBERI, Ohio
MARK R. KENNEDY, Minnesota
TOM FEENEY, Florida
JEB HENSARLING, Texas
SCOTT GARRETT, New Jersey
TIM MURPHY, Pennsylvania
GINNY BROWN-WAITE, Florida
J. GRESHAM BARRETT, South Carolina
KATHERINE HARRIS, Florida
RICK RENZI, Arizona

BARNEY FRANK, Massachusetts
PAUL E. KANJORSKI, Pennsylvania
MAXINE WATERS, California
CAROLYN B. MALONEY, New York
LUIS V. GUTIERREZ, Illinois
NYDIA M. VELAZQUEZ, New York
MELVIN L. WATT, North Carolina
GARY L. ACKERMAN, New York
DARLENE HOOLEY, Oregon
JULIA CARSON, Indiana
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
BARBARA LEE, California
JAY INSLEE, Washington
DENNIS MOORE, Kansas
CHARLES A. GONZALEZ, Texas
MICHAEL E. CAPUANO, Massachusetts
HAROLD E. FORD, JR., Tennessee
RUBÉN HINOJOSA, Texas
KEN LUCAS, Kentucky
JOSEPH CROWLEY, New York
WM. LACY CLAY, Missouri
STEVE ISRAEL, New York
MIKE ROSS, Arkansas
CAROLYN MCCARTHY, New York
JOE BACA, California
JIM MATHESON, Utah
STEPHEN F. LYNCH, Massachusetts
ARTUR DAVIS, Alabama
RAHM EMANUEL, Illinois
BRAD MILLER, North Carolina
DAVID SCOTT, Georgia

BERNARD SANDERS, Vermont

Robert U. Foster, III, *Staff Director*

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

SPENCER BACHUS, Alabama, *Chairman*

STEVEN C. LATOURETTE, Ohio, *Vice Chairman*
DOUG BEREUTER, Nebraska
RICHARD H. BAKER, Louisiana
MICHAEL N. CASTLE, Delaware
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
SUE W. KELLY, New York
PAUL E. GILLMOR, Ohio
JIM RYUN, Kansas
WALTER B. JONES, JR, North Carolina
JUDY BIGGERT, Illinois
PATRICK J. TOOMEY, Pennsylvania
VITO FOSSELLA, New York
MELISSA A. HART, Pennsylvania
SHELLEY MOORE CAPITO, West Virginia
PATRICK J. TIBERI, Ohio
MARK R. KENNEDY, Minnesota
TOM FEENEY, Florida
JEB HENSARLING, Texas
SCOTT GARRETT, New Jersey
TIM MURPHY, Pennsylvania
GINNY BROWN-WAITE, Florida
J. GRESHAM BARRETT, South Carolina
RICK RENZI, Arizona

BERNARD SANDERS, Vermont
CAROLYN B. MALONEY, New York
MELVIN L. WATT, North Carolina
GARY L. ACKERMAN, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
LUIS V. GUTIERREZ, Illinois
DENNIS MOORE, Kansas
CHARLES A. GONZALEZ, Texas
PAUL E. KANJORSKI, Pennsylvania
MAXINE WATERS, California
DARLENE HOOLEY, Oregon
JULIA CARSON, Indiana
HAROLD E. FORD, JR., Tennessee
RUBÉN HINOJOSA, Texas
KEN LUCAS, Kentucky
JOSEPH CROWLEY, New York
STEVE ISRAEL, New York
MIKE ROSS, Arkansas
CAROLYN MCCARTHY, New York
ARTUR DAVIS, Alabama

CONTENTS

FIGHTING IDENTITY THEFT—THE ROLE OF FCRA

Tuesday, June 24, 2003

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS,
AND CONSUMER CREDIT
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The subcommittee met, pursuant to call, at 10:08 a.m., in Room 2128, Rayburn House Office Building, Hon. Spencer Bachus [chairman of the subcommittee] presiding.

Present: Representatives Bachus, LaTourette, Castle, Royce, Lucas of Oklahoma, Kelly, Biggert, Toomey, Capito, Tiberi, Hensarling, Barrett, Renzi, Oxley (ex officio), Shadegg, Lucas of Kentucky, Sanders, Sherman, Moore, Hooley, Hinojosa, Lucas of Kentucky and Crowley.

Chairman BACHUS. [Presiding.] Good morning. The Subcommittee on Financial Institutions and Consumer Credit will come to order.

I want to welcome our witnesses. We have three panels today, so the hearing may be quite lengthy. This is the sixth of a series of hearings that we are having on the reauthorization of the Fair Credit Reporting Act. The preemptions or uniform standards that apply to our national uniform credit reporting act are due to expire next January 1. These hearings are being held in anticipation of either extending those uniform standards and making them permanent, or making any changes that need to be made in the Fair Credit Reporting Act to make it more friendly to consumers.

Our first five hearings have revealed without a doubt that the Fair Credit Reporting Act has led to widespread availability of credit. Those in the low-and middle-income classes have benefited tremendously from the Fair Credit Reporting Act and the availability of interest and the low interest rate in the United States. This hearing will deal with identity theft, which is I think by far the most serious problem facing Americans in their use of credit.

The hearing today consists of three panels. The first panel is made up of Federal and State law enforcement officials who will inform us about the ongoing efforts to apprehend and prosecute identity thieves. Our second panel will actually consist of two victims of identity theft. They will share their personal experiences about the crime. I very much appreciate their courage and their willingness to appear before the panel. Our final panel includes several representatives from the financial services industry. They will

share their perspective on FCRA and identity theft. We also have consumer groups represented.

Identity theft is a crime committed by individuals or organizations seeking to capitalize on the good name of an innocent and unknowing consumer. It is a particularly heinous crime in that it harms not only financial institutions, but consumers and the effect can be both widespread and last for many years. A typical incident of identity theft involves a criminal using the personal data of another individual to assume that individual's identity. Using that false identity, the criminal will obtain goods and services using the victim's credit. The identity thief may also commit additional crimes using the victim's name, creating a false arrest record for the victim, or a record of arrest by the victim for crimes that they never committed.

These activities obviously tarnish the victim's reputation, credit history and sense of security. The victim of identity theft must then make a great effort to get his or her credit report and personal history back in good shape. We sometimes refer to this as credit repair. Because the financial losses associated with identity theft are generally the burden of financial institutions and other businesses, not the consumer, financial institutions are also the victims of identity theft.

Existing Federal law does address the issue of identity theft. For example, the Identity Theft and Assumption Deterrence Act prohibits the transferring or using of another's identity for fraudulent or other illegal activities. Federal law also makes it illegal to use or traffic in counterfeit credit cards or debit cards, and prohibits criminals from attempting to obtain customer identification and other consumer information from financial institutions under false pretenses.

The FCRA also is an important tool in addressing identity theft issues. Financial institutions frequently find that the consumer reports that they obtain from credit bureaus under the FCRA provide the most useful information in attempting to distinguish the identity theft from a legitimate consumer. For example, discrepancies between an address or Social Security number contained in a consumer report and the information contained on an application can be used to identify and prevent an identity theft before it occurs. In addition, an identity thief who knowingly and willingly obtains a consumer report from a consumer reporting agency under false pretenses is subject to criminal penalties under the FCRA.

The FCRA also plays a central role in mitigating the consumer harms associated with identity theft. Under FCRA, each consumer has the right to review the contents of his or her credit report at no cost, and determine whether fraudulent activity has been attributed to the consumer's credit file. If a consumer has been a victim of identity theft which results in misinformation appearing on the consumer's credit report, the FCRA establishes a mechanism whereby the consumer can notify the credit bureau of the fraudulent information and have the information deleted.

At this time, I am going to recognize the minority ranking member, Mr. Sanders, for any opening statement that he may have.

[The prepared statement of Hon. Spencer Bachus can be found on page 70 in the appendix.]

Mr. SANDERS. Thank you very much, Mr. Chairman, and thank you for holding this important hearing, and thank you all, our panelists, for being with us this morning. We appreciate that very much.

Mr. Chairman, today's hearing will focus on identity theft. Let me just mention that on this side of the aisle, we have a number of excellent proposals that address that issue. Mr. Gutierrez, Mr. Ackerman, Mr. Ford, Ms. Hooley, and Mr. Emanuel have all brought forth some excellent ideas that I think will take us a long way in addressing the crisis of identity theft.

We all know that identity theft abuses in this country are skyrocketing. We are going to hear that from our witnesses. According to data from the Justice Department, 500,000 people, half-a-million people filed reports with law enforcement in 2002 for identity theft crimes, and an estimated 700,000 are likely to file similar reports this year. A major problem now, it is getting worse and we need some solutions to that. In addition, the dollar losses reported by identity theft victims have increased from $160 million in 2001 to $343 million in 2002. So this problem is accelerating and it is incumbent upon this committee to address it. We are going to hear, I know, in the course of the next few weeks a number of excellent ideas. I want to bring forth one idea that I think is important. That is that one very obvious and extremely helpful tool would be to provide consumers free credit reports and credit scores from all three credit bureaus at least once a year, and a description of the key factors that may have adversely affected the consumer's credit score. In other words, one way to deal with this issue and many other issues as well is to make sure that consumers all over this country have free access to their credit reports. When they have that access, they will be able to see, wow, who has been ripping me off; who has stolen my identity; and they will be able to move a lot quicker than they are at present.

I am happy to inform you, Mr. Chairman, that I have introduced legislation in this regard which is being supported by virtually all of the consumer organizations in this country, including the Consumer Federation of America, Consumers Union, and the U.S. Public Interest Research Group. Allowing consumers free access to their credit reports could substantially improve the accuracy of credit reports and cut down on identity theft. I look forward to working with you, Mr. Chairman, on this legislation.

Mr. Chairman, I would also point out a somewhat tangential issue, but important as well, that very often we will hear testimony from our friends in the banking industry and the credit card industry about this and that other matter, but I think we should be aware as we hear their testimony that in some instances at least executive compensation in the banking industry is getting really out of hand. According to an article that appeared in the Philadelphia Inquirer on June 1, 2003, "Number one on Business Week's 2020 pay scorecard was financial giant MBNA CEO Alfred Lerner with $194.9 million." Mr. Lerner died in October 2002 and was replaced in November by Charles Cawley, who managed to place number six on that list with a total pay of $48.6 million. Not too bad. Two more MBNA executives who were not CEOs also got

megabucks. John Cochran got $36 million and Bruce Hammonds, $28.6 million.

I raise this issue about excessive CEO compensation to point out that there are consumers in this country today who are being ripped off by credit card companies, who are paying up to 29 percent a year in interest rates. So when we hear our friends from the credit card companies or the banks telling us just in what kind of terrible financial need they are in, we might want to remember that number, and that the top four executives in that particular company in 2002 earned over $300 million collectively.

Mr. Chairman, the last point that I want to make on credit cards is that it is absolutely imperative that this committee address the credit card bait and switch mechanisms that some of the credit card companies are bringing forth. As we all know, the credit card industry is hooking consumers into purchasing credit cards by bombarding them, this is one of the more astronomical numbers I have ever heard. In a given year, the credit card companies send out 5 billion solicitations, 5 billion solicitations, many of them going to young people all over this country. What they promise people is low interest rates, 0 percent, 3 percent, 5 percent. What they forget to tell you is that if you borrow money on another credit card, if you were late in paying your car loan 2 years ago, your credit card rates can soar. They are ripping off the American people, and this is an issue that we must address.

Mr. Chairman, I thank you again for calling this important hearing. I am going to be running in and out because of other commitments, but I will be back. I thank you for bringing these witnesses together.

Chairman BACHUS. Thank you.

I want to especially thank Mr. Sanders, along with Chairman Oxley and Ranking Member Frank for working very closely on the FCRA reauthorization. At this time, I recognize the chairman of the full committee, Mr. Oxley.

Mr. OXLEY. Thank you, Mr. Chairman.

I will be brief and make my opening statement part of the record, but I did want to commend you for this long march through the Fair Credit Reporting Act. By my count, some 75 witnesses have testified, just about anybody that has any opinion whatsoever on FCRA has had the opportunity in your subcommittee to air their views. You deserve a great deal of credit, if nothing else but for an iron-pants performance through these long weeks of hearings that will conclude today.

We will have a voluminous record for the members to pore through and staff to pore through as we prepare to mark up legislation when we return after the Fourth of July recess. But your leadership has not gone unnoticed, and we appreciate the good bipartisan cooperation we have had on this issue. I think most of the members understand the critical importance of reauthorizing FCRA, what it has meant to our economy, that it has been one of the most successful pieces of legislation ever passed by any Congress. We want to make sure that this continues to be able to provide credit to people all over the country.

So with that, Mr. Chairman, and with my sincere thanks, I yield back.

Chairman BACHUS. I appreciate that, Mr. Chairman.

At this time, Ms. Hooley or Mr. Hinojosa, do you have opening statements?

Ms. HOOLEY. I do, Mr. Chair.

Chairman BACHUS. Okay. Ms. Hooley, you are recognized.

Ms. HOOLEY. Thank you.

Good morning. Although I have enjoyed our series of hearings on FCRA, I am excited that we are finally discussing in depth one of the core problems that has developed with our national credit system, the problem of identity theft. Identity theft is the fastest growing white collar crime in America, and legislation to correct and stem the rising tide must be enacted as soon as possible.

As you may know, the Federal Trade Commission reported that the number of persons filing complaints of identity theft with the agency nearly doubled from 2001 to 2002. A 2003 survey I recently saw found that 92 percent of Americans think it is important that the government take action on the issue of identity theft. I have been fighting to enact common sense legislation to fight identity theft for 5 years. For the first time since this struggle began, I feel the momentum is unstoppable and that legislative action on this subject is no longer a question of if, but rather of when.

We cannot and we must not ignore the fact that Americans throughout the country are begging us to act and to help them. They are begging for action sooner, rather than later. When this happens to a person, they feel violated. They are frustrated. They are angry. It takes way too long to get through the system, and many times they have a hard time just proving who they are and then it takes a longer time to get their credit report cleaned up.

Myself and Mr. LaTourette from Ohio have introduced the Identity Theft and Financial Privacy Protection Act with nearly 50 cosponsors, many of whom are sitting in this room. If this bill is enacted, it will go a long ways toward fighting the rise of identity theft. It is not perfect. I know there are other proposals that should also be enacted, but I firmly believe that every provision of this bill will enhance our citizens's security and improve our credit process. I know that Mr. LaTourette shares my conviction.

As I said, I believe the time to act is now, during our discussion of FCRA. I believe the problem of identity theft is so severe that any extension of FCRA that I support must include significant measures to fight identity theft. It seems to me there is no option. We in Congress must act this year to protect both our consumers and financial institutions from the disastrous effects of identity theft. I want to thank each of the witnesses for giving up your time today to talk about identity theft and the broader issue of reauthorization of FCRA. I look forward to continued debate on the subject and to all your comments, and to my ranking member and to the chair, thank you so much for everything you have done on this issue. Thanks.

Chairman BACHUS. Thank you.

I want to recognize the lady from Oregon, Ms. Hooley. You and Mr. LaTourette have worked with other members of this panel on identifying identity theft issue and the need for the personal information of consumers to be more secure, and to take steps in this

legislation going forward to make our ability to combat identity theft more effective.

At this time, I will recognize the gentleman from Ohio, Mr. LaTourette.

Mr. LATOURETTE. Thank you very much, Mr. Chairman.

I want to thank you very much for having this hearing today, together with the Ranking Member. I want to bring to the subcommittee's attention an individual who is going to be testifying on the second panel today, and that is Maureen Mitchell, who hails from my hometown in Madison, Ohio. I have known Maureen and her family for a number of years. As a matter of fact, her son and my daughter traversed their way through the Madison public school system together. It came as a surprise to me when in 1999 she called and said, "Steve, I need your help." It should be noted that Maureen is usually an unflappable registered nurse, a licensed realtor, and a wife and mother. It was clear to me that something serious was going on, causing her to come visit us in Painesville.

What I did not know and could not have expected was the unbelievable saga that was about to unfold for Maureen and her family. She had discovered that she was a victim of identity theft. Her determined efforts to resolve the situation through repeated calls to her creditors, law enforcement, and the FTC, credit reporting agencies were only leading her further down a downward spiral of frustration and financial strife. In the years since her first visit to my office, Maureen has testified before a number of committees here in Washington and most recently in the Statehouse in Columbus, Ohio. One of the things that I found interesting was that in some instances of identity theft you say, well, you went online and you bought something using a credit card on a computer, you had your wallet stolen or your purse stolen, or maybe somebody broke into your mailbox, but none of those items were present in Maureen's and Ray's case.

The severity of Maureen's case is what inspired me, along with my good friend Darlene Hooley, in the 106th Congress to begin working on a bill. In this Congress, it is known as the Identity Theft and Financial Privacy Protection Act. Mr. Sanders will be pleased to know that one of the provisions in that bill is in fact the provision that every consumer receive a free credit report from the agencies, and his idea has been adopted as well.

With reauthorization of the Fair Credit Reporting Act a likelihood later in this year, our committee is in a unique position to take the necessary steps to improve and continue the fight against identity theft, which is one of the fastest growing, most personally destructive and invasive crimes that can be committed against an individual. I would urge all of my colleagues to read Maureen's complete written testimony, as hers is a compelling case for this committee to act in a swift fashion. To give you some idea of the enormity of the extent that the Mitchell family has been victimized, all told it is well over $100,000. Their identities have been used to apply in a 2-hour period for $45,000 worth of personal loans at three different banks in Chicago, and they are the proud owners of two luxury sport utility vehicles, neither of which they ever purchased.

Maureen, I want to thank you for being here today and I hope that one day you will have the opportunity to visit Washington without an invitation to testify on your identity theft ordeal. Hopefully this hearing and legislation will begin to help you and the thousands of other victims of this crime get your lives back on track.

Again, Mr. Chairman, thank you for holding these hearings, and I very much look forward to hearing from our witnesses.

Chairman BACHUS. Thank you, Mr. LaTourette. You have chaired some of the hearings in this regard, and I very much appreciate that.

Let me read down through the list and see if any of the members have opening statements. This is in order of arrival. Ms. Kelly, do you have an opening statement? I also want to say that Ms. Kelly was the first member to hold hearings on information security in the House of Representatives, and we very much appreciate your early identification of the issue of identity theft.

Mrs. KELLY. Thank you, Mr. Chairman.

I really appreciate the fact that you are holding this hearing on the role of the FCRA in preventing identity theft. Earlier this year, we chaired a joint hearing together on fighting identity fraud and improving information security. In that hearing, what we learned was that identity theft is among the fastest growing crimes in America. It is a top consumer complaint according to the FTC. More importantly, we discovered that combating identity theft requires the collaborative effort of law enforcement and regulatory agencies, as well as consumers and financial institutions. All four need to be involved if we are going to stop identity theft, and all of them have to have appropriate access to appropriate information.

As this committee continues to explore the reauthorization of the FCRA, I would like to stress the impact that this law has had on our ability to combat identity theft and help the law enforcement officials in charge of tracking down illicit money get that job done. They do that job under the USA PATRIOT Act, this is one of the really positive things of the USA PATRIOT Act, and the FCRA has helped do that. The FCRA and information sharing that it has provided is essential to protecting the American people by detecting suspicious activity and weeding out the wrongdoers.

The national uniform standards under the FCRA have also facilitated a financial institution's ability to utilize additional authentications and identity verifications to protect consumer security. The protections incorporated in the FCRA are critically important in enabling victims to correct the damage to their credit histories created by identity thieves.

Over the last few weeks, we have heard testimony from many diverse panelists from lots of different witnesses endorsing the extension of the FCRA uniform standards. The Department of Treasury specifically highlighted the importance of the national credit reporting system in helping to detect identity theft, and in creating a framework for assisting its victims. I share these views and I think we have got to reauthorize the FCRA to protect Americans from really truly hideous and preventable crimes.

I thank all of the witnesses for appearing here today. I look forward to hearing what you have to say on strengthening our network to combat identity theft. But I am also pleased, and I am going to take a moment here to introduce one of the special witnesses from the great State of New York who will appear on the third panel. His name is Joshua Peirez. He is the Senior Vice President and Assistant General manager for MasterCard. Mr. Peirez is the counsel for MasterCard's North American region and he comes from my county, Westchester County in New York. It is great to have Mr. Peirez here. I look forward to his testimony and the testimony of all of the witnesses.

I thank you and yield back my time.

Chairman BACHUS. I appreciate that.

At this time, the Chairman recognizes the gentleman from Texas, Mr. Hinojosa. Also, Mr. Hinojosa, I want to say that you and I will be holding hearings Thursday on expanding consumers's rights to obtain financial services in the low-and middle-income communities, and the need of the underserved for more financial services.

Mr. HINOJOSA. Thank you, Mr. Chairman. I look forward to working with you on that hearing on Thursday.

Today, I want to thank Chairman Bachus and Ranking Member Sanders for holding this final non-legislative hearing today to investigate the role of the Fair Credit Reporting Act in fighting identity theft. It is necessary that we continue to assess the importance of the national credit reporting system. I look forward to this hearing and to hearing additional testimony to further clarify this issue.

As I noted at the first hearing, my office was contacted frequently by numerous individuals and groups about the Fair Credit Reporting Act in the first half of this year. I personally heard from industry, consumer groups and several regulators on the issue. Lately, I have not been contacted by industry groups nor consumer groups on what they would like included in the legislation that likely will be crafted and introduced in the near future. It is my hope that Treasury and the Administration will publish its long-awaited proposals on identity theft and the FCRA, perhaps as soon as this week.

Most of us realize that language has been available at the Treasury Department, but the White House has been taking its sweet time deciding what position to take on Treasury's proposal, while also watching closely the developments in the House and the hearings in the Senate. In 2001, more than 117,000 complaints from identity theft victims were added to FTC's database. In 2002, those complaints increased to almost 162,000. According to FTC Chairman Beales, the dramatic increase may reflect a growing awareness of consumers about identity theft.

Consumers who call the FTC hotline receive telephone counseling from specially trained personnel who provide general information about identity theft and help guide victims through the steps needed to resolve the problems resulting from the misuse of their identities. Consumers are advised to contact the three national consumer reporting agencies and have a fraud alert place in their file, close accounts identity thieves have accessed, dispute un-

authorized charges and report the theft to the police and get a police report.

Identity theft occurs when a consumer's Social Security number, credit card number, or name is used without his or her knowledge to open fraudulent credit, telecommunications or utility accounts, or to use already existing accounts. It can also occur when an individual's name is used unknowingly to pass bad checks or to get loans, jobs or obtain housing. This crime potentially affects every consumer in all sectors of the financial services industry, including financial institutions, credit card companies, insurance companies, mortgage companies, and hospitals. The theft can be carried out over the telephone by computer hacking into an individual's confidential files or by stealing hard copies of a company's billing information. The victim of the theft usually does not realize the information has been stolen until sometime later. As a result, these crimes could be used to support terrorism, among other criminal activities.

Today, I cosponsored H.R. 2035, the Identity Theft and Financial Privacy Protection Act of 2003, introduced by my friend, Congresswoman Hooley, the Chair of the Democratic Task Force on Identity Theft on which I serve. The Task Force investigated the exploding problem of identity theft, the fastest growing white collar crime in America, and other financial crimes. I decided to cosponsor Congresswoman Hooley's legislation because it contains strong provisions that will help fight identity theft. These provisions in this bill are extremely important to us in Texas, which ranks fifth in the number of identity theft complaints reported to the FTC.

I have said in the past that one of the main decisions we, as a Committee, needed to make is whether to extend all seven exceptions to the Fair Credit Reporting Act that preempt State law, just some of the exceptions or none of them. They all expire January 1, 2004. On June 11, 2003, I and several new Democrats cosigned a letter to Chairman Oxley and Ranking Member Frank looking towards their leadership to ensure that legislation extending the seven expiring provisions of the Fair Credit Reporting Act is passed by the House and Senate before their termination on January 1 of next year. I believe that these seven provisions enhance the efficiency of the nation's credit system, promote access to the financial industry, protect American consumers, and I am firmly committed to extending them.

With that said, Mr. Chairman, I ask that the rest of my statement be included in today's record of the proceedings.

[The prepared statement of Hon. Rubén Hinojosa can be found on page 76 in the appendix.]

Chairman BACHUS. I thank the gentleman.

I now recognize subcommittee Chairman Castle and commend him for his expertise in the matter of FCRA and your participation in these hearings.

Mr. CASTLE. Thank you, Mr. Chairman.

When they write the book about pieces of legislation not having sufficient hearings, anyone who protests that you did not have sufficient hearings, send them to me. We have had more hearings on this subject, more panels than anything that I remember since I have been in the Congress of the United States, and I came with

you, on the Fair Credit Reporting Act. And they have been informative, and I believe it has served its purpose, Mr. Chairman. I think we have a consensus forming on both sides of the aisle, now both sides of the Capitol, that extending the preemption provisions in FCRA is essential to our economy.

I am particularly interested in today's topic, the role FCRA plays in fighting identity theft because that is at the heart of people's concerns about their financial privacy. As we seek to pass legislation to extend FCRA's preemptions, we need to be careful that efforts to improve FCRA in the name of privacy do not have unintended consequences of undermining the ways FCRA currently prevents identity theft. I think today's hearing will establish the foundation we need to make sure the law of unintended consequences does not become an amendment to future legislation in the area.

I would like to mention way down on the third panel is an extraordinary Delawarean and American, Jim Kallstrom, who is now living in the State of Delaware. I think it is safe to say that when times get tough and the nation needs smart capable people to serve, Jim Kallstrom's name rises quickly to the top. In addition to his decades of service to our nation as a Marine Corps captain in Vietnam and an FBI Special Agent in Charge, Mr. Kallstrom rose to the occasion after 9-11, leaving MBNA, where he works in Delaware, to serve as the Director of public security for the State of New York. There he was responsible for counterterrorism planning and operations and served as the point of contact for the State with the then-White House Office of Homeland Security. Now Jim splits his time among advising the Governor of New York on counterterrorism, advising MBNA, and hosting the Discovery Channel weekly show, The FBI Files. So we thank him very much for being here today and look forward to his testimony, as well as the testimony of the others.

Thank you, Mr. Chairman.

Chairman BACHUS. Thank you.

Mr. Lucas or Mr. Crowley, do you have opening statements?

Mr. CROWLEY. Mr. Chairman, I do not have an opening statement. I just want to welcome someone later on as well in the second panel, Maureen Mitchell, who is nee Sullivan. She now lives in Ohio, but was originally from Woodside, Queens. Just for the record, I want to welcome her if I am not here later on.

Thank you, Mr. Chairman.

Chairman BACHUS. I thank the gentleman from New York.

At this time, it is my pleasure to introduce the gentleman from Arizona, Mr. Shadegg, and to remind members of the committee that it was Mr. Shadegg that actually introduced the Identity Theft and Assumption Deterrence Act and was the main sponsor of that legislation. So I commend you for that, Mr. Shadegg, and we welcome your participation in this hearing and your early leadership.

Mr. SHADEGG. Thank you very much. Thank you, Chairman, Bachus, for allowing me to be a part of this Financial Institutions Subcommittee hearing on identity theft. I am pleased to be here to listen to the testimony that will be provided by our distinguished witnesses.

I am particularly interested in hearing the testimony from our second panel, the victims of identity theft. I strongly believe that

we will learn the most about appropriate legislative responses from those who have experienced this crime first-hand and are intimately familiar with the difficulties victims face in trying to clear their name and repair their credit after an identity theft crime has occurred.

My personal interest in identity theft began about five years ago when two of my constituents, Bob and JoAnn Hartle of Phoenix, Arizona were the victims of identity theft. Unfortunately, Mr. and Mrs. Hartle could not be here with us today to tell their story. I am confident that we would have benefited from their experience and expertise as independent consultants to other consumer victims of identity theft. Mr. Chairman, I would like to request unanimous consent to submit for the record their written testimony.

Chairman BACHUS. Without objection.

Mr. SHADEGG. Bob and JoAnn Hartle were instrumental in getting the first State law in the nation to criminalize identity theft passed. Mr. and Mrs. Hartle suffered the devastation of identity theft when a convicted felon took Mr. Hartle's identity and made purchases totaling over $100,000. This individual also used Mr. Hartle's identity to obtain a security clearance to secure areas of Phoenix's Sky Harbor International Airport, and to purchase handguns using Mr. Hartle's clean record to get around the Brady gun law.

As a result of this victimization, Mr. and Mrs. Hartle were forced to spend more than four years of their lives and more than $15,000 of their own money to restore their credit because there were no Federal penalties for identity theft. Their case led me to introduce a bill in the House that was eventually signed into law, the bill you referenced, Mr. Chairman, the Identity Theft and Assumptions Deterrent Act of 1998. It gave law enforcement agencies the authority to investigate and prosecute identity theft crimes. Mr. and Mrs. Hartle turned their experience into something positive by establishing a nonprofit organization to assist other victims of identity theft. Their Web site, Error! Bookmark not defined., is available to provide guidance to identity theft victims nationwide. Identity theft ranges from individual instances like the Hartles involving small or large dollar amounts, to large organized professional crime rings. TriWest Healthcare Alliance, a company located in my district, may have been the victim of a professional crime ring. On December 14, 2002, computer hard drives containing their clients's sensitive, personally identifiable information were stolen from TriWest Phoenix's office.

The nature of identity theft has changed and threat is more likely than ever to come from breaches of data security. According to the Federal Trade Commission, there is a shift by identity thieves from going after single individuals to going after mass amounts of information. Law enforcement experts now estimate that half of all cases come from the thefts of business databases as more and more information is stored in computer databases that are vulnerable to attack from hackers.

The identity theft legislation that I introduced and was signed into law in 1998 was an important first step on the road to crack down on identity fraud crimes. However, Mr. Chairman, clearly more legislation is needed in this area to protect consumers from

identity theft. I am currently working on my own draft and there have been many others discussed here today, some of which have already been introduced. I look forward to hearing the testimony from our witnesses and to working with you and the other leaders in the Congress on legislation in this area.

I thank you and I yield back the balance of my time.

Chairman BACHUS. Thank you.

I would like to again thank the gentleman from Arizona for participating in our hearing. We felt like having the author of the first piece of Federal legislation to combat this problem would be appropriate, and we certainly appreciate your participation.

Mr. SHADEGG. Thank you, Mr. Chairman.

Chairman BACHUS. I think it is appropriate that with Mr. Shadegg's opening statement, I understand no other members of the subcommittee have opening statements. That being the case, I think it is appropriate for us to move to our first panel. I want to introduce them.

Mr. Howard Beales, III. Mr. Beales is testifying for the third time in our series of hearings. He is the Director of the Bureau of Consumer Protection at the Federal Trade Commission. We always find your testimony enlightening, Mr. Beales, and we welcome you back.

Mr. Daniel Mihalko, Inspector in Charge of the United States Postal Inspection Service, we appreciate your assistance with the subcommittee in preparing for these hearings. Mr. Tim Caddigan, Special Agent in Charge, Criminal Investigation Division, the United States Secret Service, we welcome you, Mr. Caddigan. And last but not least, Ms. Mary Ann Viverette, who is the Chief of Police for the City of Gaithersburg, Maryland, which is a suburb of Washington, on behalf of the International Association of Chiefs of Police. We welcome you to this morning's hearing.

Mr. Beales, if you would lead off with your testimony.

STATEMENT OF J. HOWARD BEALES, III, DIRECTOR OF THE BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

Mr. BEALES. Thank you very much, Mr. Chairman and members of the subcommittee. It is a pleasure to be back in front of you again today.

I am pleased to have this opportunity to discuss identity theft and its relationship to the Fair Credit Reporting Act. The views expressed in the written statement are those of the Commission, but my oral presentation and responses to questions are my own and do no necessarily represent the views of the Commission or any individual commissioner.

Identity theft, as you noted, can be devastating to consumers's reputations, to their financial well-being and to their sense of security. At the FTC, we are fighting identity theft on many fronts. For example, in partnership with the Justice Department and all of the agencies that are represented at this table, the Postal Inspection Service, the Secret Service, and the International Association of Chiefs of Police, we are training local law enforcers on how to fight identity theft. Today, we are holding a training session in Westchester, New York.

We at the FTC are also providing law enforcers with case referrals from our identity theft data clearinghouse. We are also working to keep consumers' financial data safe through our new safeguards rule, which took effect at the end of May, and our enforcement actions against companies that fail to keep their security promises to consumers. Just last week, we announced a settlement with online retailer Guess.com for failing to protect customer data as promised. We also released a tip sheet for businesses on the steps they should take to assure the security of their online systems.

Through workshops, educational campaigns and our ID theft hotline, we are counseling consumers and businesses on how to prevent identity theft. We are also providing consumers with tools such as our uniform identity fraud affidavit to help them recovery more quickly and easily from identity theft.

Today, you have asked for testimony about identity theft in the Fair Credit Reporting Act. In addition to harming consumers, identity theft threatens the fair and efficient functioning of consumer credit markets. It undermines the accuracy and credibility of the information flows that support those markets. Credit bureaus are simultaneously a target for identity thieves and a valuable resource for combating identity theft. The credit reporting system can play an important role in helping to detect identity theft, in limiting the damage from identity theft, and in helping victims to clean up the mess that thieves leave behind.

The Fair Credit Reporting Act helps consumers detect identity theft by providing consumers access to credit reports when they need them most. A credit report digests in one timely document all accounts opened in the consumer's name, and it is the best way to discover those accounts that may have been opened by an impostor. Under the FCRA, consumers who believe they may have fraudulent information in their files are entitled to a free credit report.

Moreover, the FCRA requires that consumers who are denied credit based on information in a credit report be notified of the adverse action and given the opportunity to obtain a free copy of the credit report. This adverse action notice can alert consumers that they may have bad marks on their credit record that they do not know about. The free credit report helps them to pinpoint the fraudulent or erroneous accounts. Adverse action notices provide consumers with a critical safeguard and we are vigorously enforcing the FCRA's adverse action provisions.

In addition to helping victims detect identity theft, the credit reporting system helps limit the damage that identity thieves can cause by allowing for the placement of a security alert in a victim's credit file. Currently, the three major credit bureaus include a standardized format security alert in the credit reports of identity theft victims. This alert puts potential creditors on notice that they should proceed with caution when granting credit in the victim's name.

Finally, the credit reporting system can help identity theft victims clean up the bad credit marks caused by a thief. A common problem of victims is that they find it difficult to get credit, insurance or employment in the wake of an identity theft incident because the impostor has damaged their credit history. The big three

credit bureaus now allow victims to block fraudulent information on their credit report with a valid police report of the identity theft incident.

We are working with the credit bureaus to develop other victim assistance programs. For example, this spring the credit bureaus implemented their joint fraud alert initiative whereby victims only need to call one credit bureau to get a security alert and a free credit report from all three. These and other kinds of steps can help to reduce the costs and the consequences for identity theft victims, but there is clearly more to be done.

I thank you for the opportunity to appear today. I look forward to responding to your questions.

[The prepared statement of J. Howard Beales III can be found on page 87 in the appendix.]

Chairman BACHUS. I appreciate that.

Mr. Mihalko?

STATEMENT OF DANIEL L. MIHALKO, INSPECTOR IN CHARGE, CONGRESSIONAL & PUBLIC AFFAIRS, UNITED STATES POSTAL INSPECTION SERVICE

Mr. MIHALKO. Thank you, Mr. Chairman. Good morning, members of the subcommittee. On behalf of the Postal Inspection Service, I would like to thank you for holding this hearing and giving me the opportunity to discuss identity crimes and the significant role the Postal Inspectors play in combating it.

To put things in perspective, I would like to start by talking about three things: the mail, the Postal Service and identity crimes. The Postal Service delivers about 200 billion pieces of mail each year. In this country, there is an expectation that each one of those pieces is going to get delivered not only in a timely manner, but it is not going to be tampered with, no one is going to take anything out of it, no one is going to read the correspondence. The responsibility for safeguarding those 200 billion pieces of mail rests with the Postal Inspection Service.

As Federal law enforcement officers, we ensure the confidence in the mail by enforcing over 200 Federal statutes that deal with the mail. Primary among those are the theft or possession of mail and the oldest and the still most effective consumer protection law, the mail fraud statute. Last year, Postal Inspectors made over 11,000 arrests, 6,000 of those were for mail theft. Of those 6,000, 2,000 were for identity theft crimes. In fiscal year 2003, we have already surpassed that number of identity theft arrests.

I think this morning we have already heard some good explanations and definitions of what identity theft is and the way it occurs. Over the years, Postal Inspectors have developed an expertise in working these types of cases, particularly when they involve the use of the mail. Those that involve the use of the mail receive swift action by Postal Inspectors. We work hard to ensure consumers are being protected. In addition, we work closely with the mailing and the financial industry to develop guidelines on how best to design mailing pieces to prevent theft. This partnership illustrates how the industry as a whole is serious about the issue. Mail is very important to consumers who receive it, and it is very important to the businesses that send it.

I am sure all of you have received preapproved credit applications in the mail. Those mailings were prime targets for an identity thief because they simply required a signature and the return of the form back to the company. When stolen from the mail, the thief could redirect the response to the application to a different address and have the credit card sent there. But times have changed due to our efforts and industry awareness. For example, credit card companies have adopted our security recommendations and now automatically discard applications when they are returned with a change of address, making them less attractive to the identity thief. Also, industry has changed its practices. Credit offers now contain much less information.

Fraudulent changes of address sent through the post office used to be another favorite vehicle for identity thieves, but not anymore. The proactive effort by the Postal Service to prevent false changes of address is the move validation letter. When a change of address is filed now, the Postal Service sends a letter to both the old and the new address. The letter instructs the individual to call an 800 number if they have not filed the change of address. This simple measure has virtually eliminated the placing of false change of addresses with the Postal Service as an avenue for committing identity theft.

As we have made it more difficult for mail theft to be a component of identity theft, the crime has evolved to the Internet and other electronic means. Personal information contained in corporate and government records and computer databases is a fertile area for dishonest employees working in conjunction with identity thieves. Businesses understand the need to protect their personal data. Improved data security should be a goal of all businesses. We can measure arrests and the effectiveness of law enforcement efforts, but it is hard to measure the full impact on victims, and it can be devastating. I am sure you are going to be hearing about that in your second panel when the victims testify. A couple of interesting points, most victims do not learn about the theft of their identity until 14 months after it has occurred. It generally takes about 44 months to clear up their cases, and victims report that they spend on average 175 hours actively trying to restore their credit rating and to clear their good name. Victims run the gamut of society. They are wealthy; they are poor; they are old; they are young. No one is immune and everyone is a potential victim.

Our experience has shown that enforcement laws coupled with an aggressive education campaign, the cooperation of industry and the interagency enforcement efforts are invaluable tools in the fight against identity crimes. In addition to modifying industry practices and making financial mailings less attractive to a thief, our partnerships have resulted in a number of fraud prevention guides. The first one is Identity Theft, Safeguard Your Personal Information. This is a Postal Inspection Service publication we first put out in the late 1990s. As of this point, we have printed and distributed over 2 million of these guides to businesses and consumers.

Second is a video called Identity Theft, The Game of the Name. This is a video that is put out for law enforcement, for consumer groups, and for corporate personnel. It talks about the dangers of identity theft and some prevention tips. Another guide that we put

together is Detecting and Preventing Account Takeover Fraud, a publication which goes towards credit grantors with information for preventing takeover schemes. Later this year, the joint law enforcement-financial industry task force called the Financial Industry Mail Security Initiative will issue a book on best practices developed over the years.

As Congresswoman Kelly said, aggressive law enforcement efforts are not enough. They are a key component of our mission, but arrests are not the only solution. We have found that creating awareness and prevention programs for consumers can go a long way to lessen the impact this crime has on the public. In addition to the two brochures and the videos mentioned, we partnered with Showtime network in 2000 to produce a Showtime movie on television about identity theft based on cases of Postal Inspectors. This past year during national consumer protection week, Postal Inspectors partnered with the Postal Service's consumer advocate in a nationwide awareness campaign on identity theft. This September, the Postal Inspection Service, along with our partners the FTC and the Postal Service, will be unveiling yet another nationwide campaign. This one is also on identity theft.

This year, we are going to take a two-pronged approach. We are going to be providing information to consumers as we have in the past, but we are also going to be addressing businesses on the need to safeguard their files and databases of customers' information. Actor Jerry Orbach of television's Law and Order fame, who also was a victim of identity theft, has agreed to be the campaign spokesperson. The campaign will include a mailing to residences in 10 States identified by the FTC as reporting the most identity theft complaints, a public service announcement featuring Jerry Orbach, and an identity theft insert outlining prevention tips that will be included with monthly financial industry statements. We will be displaying in lobbies in all 38,000 post offices, which is going to make people aware of identity theft and some of the prevention tips. We are also going to produce another informational video and we are going to place half-page newspaper ads in the major newspapers in the 10 States that the FTC identified as having the most complaints.

The Mullen agency of Pittsburgh has provided support for this campaign on a pro bono basis, but what really makes this campaign unique is the funding source. We have all heard the saying, "crime does not pay." Well, in the case of this awareness case, it does pay. This campaign is being funded through a unique application of fines and forfeitures paid by criminals in a past fraud case.

Educating the public and working to reduce opportunities where the Postal Service and the mail can be used for illegal purposes are crucial elements in our fight against identity crimes. As always, we will do our part to remove criminals from society. We appreciate the subcommittee's recognition of the importance of this issue.

Thank you, Mr. Chairman.

[The prepared statement of Daniel L. Mihalko can be found on page 165 in the appendix.]

Chairman BACHUS. Thank you.

Special Agent Caddigan?

STATEMENT OF TIM CADDIGAN, SPECIAL AGENT IN CHARGE, CRIMINAL INVESTIGATIVE DIVISION, UNITED STATES SECRET SERVICE

Mr. CADDIGAN. Mr. Chairman, Mr. Sanders, thank you for inviting me to be part of this hearing today and the opportunity to address the committee regarding the Secret Service's efforts to combat identity crime and protect our nation's financial infrastructure.

The explosive growth of identity theft-related crimes has resulted in the evolution of the Secret Service into an agency that is recognized worldwide for its expertise in the investigation of all types of financial crimes. Our efforts to detect, investigate and prevent financial crimes are aggressive, innovative and comprehensive. The burgeoning use of the Internet and advanced technology, coupled with increased investment and expansion, has intensified competition within the financial sector. Although this provides benefits to the consumer through readily available credit and consumer-oriented financial services, it also creates a target-rich environment for today's sophisticated criminals, many of whom are organized and operate across international borders.

Identity crime is not targeted at any particular demographic. Instead, it affects all types of Americans regardless of age, gender, nationality or race. What victims do have in common is the difficult, time-consuming and potentially expensive task of repairing the damage that has been done to their credit, their savings and their reputation. According to the GAO, the average victim spends over 175 hours attempting to repair the damage inflicted by identity crime.

Identity crimes originate when another person obtains your personal or financial identifiers. Methods of acquiring such information range from the so-called "dumpster diving" where the criminal searches through your garbage for billing statements or other documents that may include personal identifiers, to insiders who purge information from their own company's database and place it for sale on the Internet.

Since our inception in 1865, the twin pillars of the Secret Service have been prevention and partnership building. A central component of the Secret Service's preventive effort has been to increase awareness of issues related to identity crime, both in the law enforcement community and among the general public. The Secret Service has undertaken a number of unique initiatives aimed at increasing awareness and providing the training necessary to combat identity crime and assist victims in rectifying damage done to their credit. This includes the development of a number of training tools designated to assist our local law enforcement partners.

Mr. Chairman, I cannot emphasize enough the importance of sharing expertise with our local and state police partners, and empowering them with the ability to respond on the local level to identity crimes. In a nation of thousands and thousands of communities and a population exceeding 270 million, providing the first responder, in this case a local police officer, with the training and information they need to investigate an identity crime and provide victim assistance, is imperative.

We believe the Secret Service can best service the American people by acting as a force multiplier. In other words, directing our ef-

forts towards providing the 700,000-plus local and State law enforcement officers with the tools and resources they need to provide assistance in their communities. In partnership with the International Association of Chiefs of Police, the Secret Service produced the best practice guide for seizing electronic evidence. This pocket-sized guide instructs law enforcement officers in the seizure of evidence, from personal computers, wireless telephones, to digital cameras. We have also worked with this group and our private sector partners to produce the interactive computer-based training program known as Forward Edge, which incorporates virtual reality features and technical support to instruct local law enforcement officers on how to address an electronic crime scene.

Thus far, we have distributed free of charge over 300,000 best practice guides and over 20,000 Forward Edge CDs to State, local and Federal law enforcement officers. In addition, we are nearing completion of an identity crime video and CD-ROM which will contain over 50 investigative and victim assistance resources that law enforcement officers can use when combating identity crime. In the coming weeks, we will be sending an identity crime CD-ROM to every law enforcement agency in the United States. Over 25,000 identity crime CD-ROMs are being prepared for distribution.

In short, any police department in the country, regardless of size or resources, now has access to state-of-the-art training as well as multiple investigative and victim assistance resources to help them combat identity crime. In a joint effort with the Postal Inspectors, the FTC, the Department of Justice and the International Association of Chiefs of Police, we are hosting identity crime training seminars for local law enforcement. In the last year, we have held such training seminars in Chicago, Dallas, Las Vegas, Des Moines, Washington, D.C., and Phoenix, and seminars are planned in the near future for Washington State and Texas. One, as previously reported, is ongoing in New York State as we speak.

For law enforcement to properly prevent and combat identity crimes, steps must be taken to ensure that State, local and Federal agencies are addressing victims' concerns in addition to actively investigating identity crime. It is essential that law enforcement recognize that identity crimes must be combated on all fronts, from the officer who receives the victims's complaints to the detective or agent investigating an organized identity crime ring. The Secret Service is prepared to assist this committee in protecting and assisting the people of the United States with respect to prevention, identification and prosecution of identity criminals.

Mr. Chairman, that concludes my prepared remarks. I am happy to answer any questions your or the committee members may have.

[The prepared statement of Tim Caddigan can be found on page 100 in the appendix.]

Chairman BACHUS. Thank you, Agent Caddigan.

At this time, we will hear from Chief of Police Viverette.

STATEMENT OF MARY ANN VIVERETTE, CHIEF OF POLICE, GAITHERSBURG, MARYLAND, ON BEHALF OF THE INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

Ms. VIVERETTE. Good morning. I am pleased to be here this morning on behalf of the International Association of Chiefs of Police.

As I appear before you today, the issue of identity theft is one of great and growing concern to the law enforcement community. In a relatively short period of time, identity theft has transformed from a relatively unnoticed crime to a major problem in the United States and around the world. In the last few years, personal information has become one of the commodities most sought after by criminals in this country and elsewhere.

Although identity theft is in itself a criminal act under both Federal and most State laws, the theft is almost always a stepping stone to the commission of other crimes such as credit card, bank, computer and Internet fraud, designed to enable the perpetrator to profit from the original theft. Furthermore, funds obtained illegally as a result of the identity theft and its resultant frauds may be used to finance other types of criminal enterprises, including drug trafficking and other major forms of criminal activity. As the use of technology to store and transmit information increases, so too will identity theft.

The ability to accurately define the financial losses of the vast number of crimes committed by means of identity theft is not possible at this time. Many identity theft crimes are not reported to the police and there is no single source of information on this issue. It is fair to say, however, that the cumulative financial losses from identity theft and various crimes that feed from it are staggering. However, perhaps even more tragic than the monetary loss, is the personal cost of identity theft. Because identity theft by definition involves the fraudulent obtaining of funds in the name of someone else, the victim of identity theft may sustain not only great financial loss, but also severe damage to credit standing, personal reputation and other vital aspects of the victim's personal life. Even if the victim ultimately clears his or her credit records and avoids other personal and financial consequences of identity theft, the physical and mental toll on the victim can be significant.

Identity theft is not perpetrated only by so-called "white collar" thieves. It is committed by criminals of all types. A recent report indicated that during the period of November 1999 to March 2001, about 12 percent of all suspected perpetrators had a personal relationship of some sort with the victim. However, the remaining 88 percent of suspects had no relation to the victim of the theft. In most cases, the thieves are geographically located far from the victim's place of work or residence. These perpetrators may be solo operators, but more often are members of a larger criminal organization. Such organizations may be local, regional, national or international.

In early years, the involvement of local police departments in identity theft cases was typically minimal. In fact, many local police departments did not know how to respond because the crime was not well understood. This was caused by several factors, including the lack of State laws making identity theft a crime, the

fact that most identity theft operations are multi-jurisdictional enterprises with perpetrator and victims usually widely geographically separated, and the general lack of police expertise in investigating the crime of identity theft.

Fortunately, the situation is now rapidly being remedied. The passage of numerous Federal and State statutes has given law enforcement agencies the authority to investigate and prosecute identity theft crimes and departments everywhere are becoming more aware of the significance of identity theft and the availability of a means to combat it. Effectively combating identity theft will require not only the dedication of significant resources and personnel, but also greater collaboration and cooperation between Federal, State, tribal and local law enforcement agencies. This information-sharing among agencies is essential as it may not only lead to successful prosecution of the case in one jurisdiction, but concurrent investigations in other areas of the country. I am pleased to say that in recent years law enforcement agencies have made significant strides in this area, and are increasing our capability to investigate, track, apprehend and prosecute these criminals.

Nevertheless, the law enforcement community cannot effectively combat identity theft by itself. Citizens need to take proactive steps to protect their personal information. Businesses must act to establish safeguards that will ensure that the personal information of their patrons is not exposed. Policymakers at all levels of government need to review current statutes to ensure that protection of personal information is a priority and develop legislation that will strengthen the penalties for identity theft. Only by acting to establish greater protections of personal information and by aggressively tracking down and punishing those who commit identity theft can we hope to turn the tide in this battle.

Thank you, Mr. Chairman.

[The prepared statement of Mary Ann Viverette can be found on page 202 in the appendix.]

Chairman BACHUS. I appreciate the testimony of the panel.

At this time, I recognize the members for questions. The gentleman from Pennsylvania, Mr. Toomey?

Mr. TOOMEY. Thank you very much, Mr. Chairman.

I appreciate the testimony we have just heard. It is focused largely on enforcement of existing laws, which is obviously a very important part of this. But I was hoping that several of you might comment on whether better law enforcement, better training, more resources, more education, is that really likely, in your judgments, to reverse this really shocking trend that we have had, this big acceleration, this upward spike in the frequency of identity theft? Is better enforcement of existing law going to be sufficient to reverse this trend, in your minds, or do we need something above and beyond, in addition, or separate and apart from that?

Mr. Beales, perhaps you would like to begin?

Mr. BEALES. I think we need to address the problem on many fronts. I think enforcement is a key part of any attempt to solve it. I think better penalties would be something that would certainly help and would enhance the enforcement effort. I think there are probably also things that can be done to help with prevention of the crime in the first place and to help victims recover more easily.

We at a staff level are hard at work on a package of recommendations that we would bring forward to the commission and then to the Congress, but at this point we do not have any other recommendations.

Mr. TOOMEY. Anyone else care to comment?

Mr. MIHALKO. Yes, I would like to comment.

Resources are always an issue. We in law enforcement never have enough to go around. We do have plenty of good statutes, though, at least in the Postal Inspection Service. We have statutes that cover identity theft on both ends. If there is a theft of mail, we have excellent Federal statutes to deal with theft or possession of stolen mail. If the mail is not part of the initial scheme, but is then used to either mail a phony credit card or a counterfeit credit card, whatever it may be, we have an excellent statute there with the mail fraud statute.

I think what we need, and what I hear from a lot of my inspectors out in the field, is that we need more resources for prosecutors. There seems to be a shortage of Federal prosecution of the identity theft-type cases. But like Mr. Beales said, we also agree that prevention and educating the consumer is a key component of fighting this crime. We just can't seem to get enough education out to people.

Mr. TOOMEY. I would like to follow up on the prevention idea, because it seems to me there are different orders of magnitude of identity theft. Someone can grab a credit card carbon out of a wastebasket and identify my credit card number and perhaps run up some charges. That is a terrible thing, obviously. It is a serious crime, but it is something that I am likely to discover relatively quickly and I am likely to be able to avoid actually incurring the expense. The more serious types of crimes, of course, are those when someone establishes an identity, steals my identity, establishes accounts, obtains credit through this new bogus identity, and then might run up huge credit obligations, which I discover much, much later, which are a huge problem now.

Are we doing enough to prevent that from happening? Are there more things that ought to be done by the private sector to prevent those kinds of abuses? I see, Officer, you are nodding your head. Do you have a response to that?

Mr. CADDIGAN. I think we have seen in recent years the private sector and law enforcement come together on this issue. That has been tremendously beneficial to the consumer. I see the credit card companies, they not only share information among themselves, but with law enforcement. I see all law enforcement, State, local and Federal, coming together and sharing resources. State prosecutors are working with Federal prosecutors. It is not a crime that is going to be completely eliminated overnight, but from our perspective we do see growth in cooperation on all fronts, as Mr. Beales has said, that we have prevention, we have education, we have awareness.

One of the areas that we are most concerned about is information security with regard to end-users and consumers. That is something that is taking a higher priority because when we do have, for example, a hacking situation, customer databases are stolen in bulk, that has a tremendous impact on the identity crime

arena. When we can deal with end-users on how to safeguard their systems and safeguard their data files, that is going to be a huge impact. Those relationships are being built as we speak. Those conversations are being had at all levels with regard to security, information sharing and safeguarding information sharing. So I think from our perspective, that multi-front process is effective and it does handle not only the simple carbon theft, but it also deals in the international Internet theft or hacking case involving a large magnitude of identity crimes.

Mr. TOOMEY. Does anybody else have a comment?

Ms. VIVERETTE. Yes, sir. Local law enforcement is really overwhelmed with investigating these, so I agree that prevention is part of the way to solve this. There are several recommendations by the investigators that look into these cases every day. One of those is the availability of instant credit tends to be a problem. They recommend requiring thumbprints or digital photos with any credit application.

Mr. TOOMEY. So some kind of system for authenticating the applicant?

Ms. VIVERETTE. Yes, sir. And the addition of possibly a PIN number along with the credit card to additionally verify the user as the proper person.

Mr. TOOMEY. Thank you very much.

Thank you, Mr. Chairman.

Chairman BACHUS. I thank the gentleman from Pennsylvania.

At this time, the Ranking Member, Mr. Sanders, is recognized.

Mr. SANDERS. Thank you, Mr. Chairman. A question for Mr. Beales, to begin with. Mr. Beales, in your oral statement, you mentioned that when consumers discover that they are victims of identity theft, they may receive a free copy of their credit report. In your judgment, wouldn't it be a good idea if all consumers were to get a free copy of their credit report to catch identity thieves quicker and correct errors in a prompt manner? In other words, if people were able to gain access to their reports, they would see aberrations and dishonest dealings. Does that make sense to you?

Mr. BEALES. The Commission has not taken a position on that. I think that there is no question that access to the credit report would help. I think under the existing statute, consumers have access to a free credit report when they are most likely to need it, which is when they think there is fraudulent information or when they find out that there is a problem.

Mr. SANDERS. I understand that. In general, given the significant increase in this horrendous type of crime, if people receive the reports, they would be able to spot the problem a lot quicker than is currently the case right now. I think one of the problems that we are hearing is that people do not know that they are being ripped off for, in some cases, a relatively long period of time. Don't you think this would expedite the process?

Mr. BEALES. I think it certainly could.

Mr. SANDERS. Okay. Thank you.

Mr. Caddigan, do you have thoughts on that?

Mr. CADDIGAN. I would agree that anything that would make the consumer more aware of his current situation is a preventive tool.

Mr. SANDERS. Okay. Thanks.

Let me ask Chief Viverette a question. You may not want to answer it. It may be too political, but that is okay. One of the debates, the key debate that is going on here has to do with Federal preemption. Some of us believe that we should have very strong standards for identity theft and other consumer problems in general at the Federal level, but we should allow States to go forward in a more aggressive way if they want to. In fact, Maryland, as I understand it, is one of six States in the country right now which does require free credit reports. Is that correct?

Ms. VIVERETTE. I believe it is, yes, sir.

Mr. SANDERS. Okay. Now, I am not suggesting that Congress would take away Maryland's right to do that. I doubt that they would. But give us your thoughts about a State that has been proactive in trying to protect consumers, should States in your judgment continue to have that right?

Ms. VIVERETTE. The decision of the International Association of Chiefs of Police is normally to keep the rights at the State level. Yes, sir.

Mr. SANDERS. Okay. Thank you.

Mr. Chairman, what you heard is from attorneys general from all over this country who believe that they should have the right to be aggressive in protecting consumers, and you are hearing from police officers as well, who want strong consumer protection. I would note the point that the chief made a few moments ago, which is a very important point. I am sure it is all over this country that local law enforcement is being overwhelmed. When somebody calls you up, that takes a heck of a lot of resources to address that problem. Is that correct, Chief?

Ms. VIVERETTE. Yes, sir.

Mr. SANDERS. All right. So I would suggest, Mr. Chairman, that we want to be as aggressive as we can. One way that we are aggressive is allowing States to go further than the Federal government.

Thank you, Mr. Chairman, and I thank the panelists.

Chairman BACHUS. Thank you, Mr. Sanders.

Ms. Kelly?

Mrs. KELLY. Thank you, Mr. Chairman.

Mr. Beales, you said that there can be some things done to help with prevention. Would you mind just expanding on that a little bit? You made the remark and then went on with something else.

Mr. BEALES. We are working on trying to develop and to analyze legislative ideas that we would recommend to the commission and then the commission would offer its advice if that was appropriate to you all. I think the one active prevention program that I think really should be seen as a prevention program that we are very much involved in now and should be continued is efforts to protect information security. Increasingly we see that as the source of the information that turns up in identity theft cases, and we see, frankly, very many businesses that have not taken basic precautions to protect the security of their information.

We have brought cases in some of those instances, our guest case, that I mentioned, which involved the failure to close a well-known vulnerability in a system. And we have developed a business education pamphlet to encourage businesses to look for those

kinds of known vulnerabilities and to fix them. I think that is an important preventive effort and I think there is more that can be done in that area in particular.

Mrs. KELLY. One of the reasons that I am concerned about this is that we heard testimony just now about educating the consumer, but any more the way that identity theft can happen, there isn't any act that the consumer does necessarily. It is not about just making sure you tear up your credit card slips when you throw them out. Your identity can be stolen without your knowledge by your not doing anything at all different than you have ordinarily done. That is really tough to educate about. People, I think, are very vulnerable and you can educate them to do certain things, but there are limits to what we can do to educate people to protect themselves.

I am wanting to know what kind of things we are doing with regard to identity theft and terrorism, the movement of terrorism money. We know that that has occurred. I really would like to ask Mr. Caddigan, could you talk to me a little bit about what the Secret Service is doing to put a check on identity theft or identity use in transferring terrorism's money?

Mr. CADDIGAN. When we talk terrorism, the FBI has always taken the lead in the terrorism investigations. That includes the financial investigations. We are an active participant in their initiatives through their JTTFs across the country. So what we try to do is to bring our expertise to bear in the financial sector and apply them to ongoing initiatives that we have in tracking terrorism in our country. That may apply to passport fraud or counterfeit documents, to credit cards that were used to fund individuals that are staying here. It does run the gamut with regard to our own agency's initiatives. We do that under the umbrella of a joint initiative led by the FBI.

Mrs. KELLY. Maybe you and I can explore that in a little less public venue, but I am very interested in what you are doing. This takes me to another level, and that is with anything that we do with regard to protecting people's identity and anything that you do with regard to helping share information so that people can have identity protections, that sharing of information steps into another field, and that is the privacy issue. I wonder if anyone on this panel would be willing to address the problems we are going to experience as we get deeper and deeper into the protections with regard to privacy.

Mr. Beales?

Mr. BEALES. I think that one of the great successes of the Fair Credit Reporting Act is the way in which it balances those concerns, the tremendous benefits of information sharing in detecting and preventing and mitigating the consequences of bad credit and of identity theft, and at the same time protecting privacy. It does that by restricting uses to people who have a permissible purpose and by trying to assure that the information is accurate and that the consumer has a way to try to correct it if it is not. But I think privacy is an important component of it and is really sort of a key goal of the Fair Credit Reporting Act.

Mrs. KELLY. Anyone else want to pick up on that? Thank you very much. My time is up.

Thanks, Mr. Chairman.

Chairman BACHUS. Thank you.

Mr. Hinojosa?

Mr. HINOJOSA. Thank you, Mr. Chairman.

I want to ask a question of Mr. Beales. Did you answer the question about or the idea that was given by Mr. Sanders, providing consumers with a free credit report annually or biannually at their request?

Mr. BEALES. The Commission has not taken a position on that. I think that the consumers have credit reports at the time they are most likely to need it, at the time it is most beneficial, which is when they think there is fraud or when there has been an adverse action. But I think there is no doubt that more availability of credit reports would help in combating the problem.

Mr. HINOJOSA. I disagree that you would wait until you are applying for credit to buy a car a house or whatever, because all the testimony says that most consumers do not find out until about 14 months after the occurrence of that identity theft. So it seems to me that we are going to have to address that question and see what the costs would be and if it is feasible.

I would like to ask Mr. Caddigan the question that I had on trying to give training to our officers out in the field. It seems to me it is time-consuming, but very important. The question is, do you know if the FBI or Secret Service agencies, are able to reach large numbers of officers in States like Texas and California?

Mr. CADDIGAN. A program that is ongoing right now in the State of New York is a collaboration with all four partners at the table here today. We are able to reach across all law enforcement, to include the financial institutions, anybody that would have a need to provide assistance in the area of identity theft, whether it is criminal or victim assistance. The event today has several hundred officers there representing dozens and dozens of departments in New York. We think that by being able to provide a Federal, State and local perspective to the problem and solutions. We are not there just to identify a problem. We are there to provide you with skill sets in providing real solutions to your community or your constituency on how to deal with this epidemic.

So when we can reach out to a victim and make them aware of what they need to do to safeguard themselves, not only from crime that has already occurred, but for future crime that potentially could occur, we feel that that force multiplier in the law enforcement community has a ripple effect that is a substantial benefit in this initiative.

Mr. HINOJOSA. I understand what you said, Mr. Caddigan. Possibly my question, then, should go to Chief Viverette. What I heard Caddigan say is that they were training the trainers, 100 of them in New York. I am talking about reaching much larger numbers. Could it be done through, say, video conferencing? Could it be done through distance learning like the universities are doing now where you could have multiple sites listening to the presentation? If that is so, if it is possible, how do chiefs of police give release time to large numbers of officers so that they can be trained?

Ms. VIVERETTE. Sir, the CD-ROM that the Secret Service has put together is an excellent resource for local law enforcement. Most of

us have training commissions at the State level that can require training. The CD-ROMs are perfect for roll-call training at the beginning of a shift. And generally what we are doing is making the patrol officer aware of what is out there, their resources. They will never have the time to do the follow-up. So we are training investigators at a higher level and the patrol officer is provided the resources to know where to go to follow up on their report.

Mr. HINOJOSA. I am concerned that the numbers of identity theft complaints are increasing rapidly, which means that there is insufficient dissemination of information and education to the public and those that help us. The chiefs of police and their officers are evidently not getting enough training or resources to get it done.

So the last question that I would have, Mr. Chairman, is to Howard Beales. Do you support Mrs. Hooley's legislation on identity theft?

Mr. BEALES. The Commission has not taken a position on that legislation. I think there are a number of features in that legislation that are attractive, but the Commission has not at this point taken a position.

Mr. HINOJOSA. We are going to go into a debate on that proposal. I hope that all four agencies would take a good close look because we really need to stop this increase that is occurring and being reported, and it is going to be very important that we get the help of all four agencies.

With that, Mr. Chairman, I yield back the rest of my time.

Chairman BACHUS. Thank you.

The gentleman from Texas, Mr. Hensarling?

Mr. HENSARLING. Thank you, Mr. Chairman.

I think one thing we can all agree on is that identity theft is a very serious and pervasive crime in the U.S. I myself at an earlier hearing announced that I had been victimized by identity theft prior to coming to Congress, when I was a small businessman and a former employee managed to open up a credit card in the name of my small business. When I discovered it, there was about a $22,000 tab on the credit card that had not been paid. Fortunately for me, with one telephone call and one letter, I was able to take care of the matter, so I can attest, at least in my case, occasionally the system does work.

The question really for us today, though, as we look at the title of this hearing, is fighting identity theft, the role of FCRA. So really to cut to the chase, I am interested in the opinion of the panelists, is FCRA friend or foe? Besides the good that comes from FCRA, and we have heard some very persuasive testimony about how we in America enjoy the greatest availability of credit, the lowest-cost credit in the world, and that FCRA plays a very significant role in that. But the question today is, when it comes to identity theft, are we better off having a paradigm that gets us closer to a national standard of credit reporting with a central database, or are we better off with more of an individualized state patchwork system, just with the narrow question of combating identity theft?

Mr. Beales, if we could start with you and receive your opinion on the matter.

Mr. BEALES. I think the uniform system and the safeguards of the Fair Credit Reporting Act do help to reduce the risk that credit

bureaus and credit data are the source of identity theft. The fact that the data is centralized and largely in three large institutions I think facilitates efforts to protect the data and facilitates efforts to prevent unauthorized access and to control access, compared to lots of little databases in lots of different places.

Mr. HENSARLING. Mr. Mihalko?

Mr. MIHALKO. I think a national standard is a huge benefit for Federal law enforcement, if we only have to deal with one type of standard. It is also a big benefit for the mailing industry so that they only have to deal with one standard nationwide and do not have to deal with 50 different standards in their mailings across the borders.

Mr. HENSARLING. Mr. Caddigan?

Mr. CADDIGAN. From a Federal law enforcement agency, any standard that eliminates confusion is best for us as we cross State lines in our investigations. The sharing of information with regard to verification check and balance is something that I think will show leads to a reduction in identity crimes. It provides earlier response to potential problems.

Mr. HENSARLING. Ms. Viverette?

Ms. VIVERETTE. Yes, sir. I agree with Mr. Caddigan. It is a situation where when we cross State lines, that is where as a patrol officer we have problems with the follow-up on the investigations. So his remarks are appropriate.

Mr. HENSARLING. We have heard advocacy about a proposal to ensure, I suppose, that all American citizens receive a free copy of their credit bureau reports. Mr. Beales, my guess is you are the expert on this subject, but I am under the impression that free reports are made available already today, for example, to the indigent, to those who have been denied credit, and to those who believe they have been a victim of identity theft. Is my understanding correct?

Mr. BEALES. There are free reports available to people who think they are victims of fraud. There are free reports available to the indigent and the unemployed. There are free reports available to anybody if there is an adverse action taken based on information in the report. Those are the circumstances and in some of those, I think, are the circumstances where the report is most valuable, but it could have value in other circumstances as well.

Mr. HENSARLING. My guess is no one on the panel is qualified to come up with a cost estimate of what that proposal would indeed cost the system. I am just curious what impact that might have on our credit availability and our credit costs should such a plan be enacted.

I see my time is out, Mr. Chairman.

Chairman BACHUS. Thank you.

Mrs. Hooley?

Ms. HOOLEY. Thank you, Mr. Chair.

I have a question for the entire panel, and I apologize for not being here the entire time, and hopefully you have not answered this question yet. One of the things we talk about when we look at identity theft is it is really composed of five pieces, and one of the pieces is prevention; it is education; it is how do you get through the process; it is how do you leave room for technology to

help solve the problem. And the last piece, and a very important piece, is law enforcement.

I have spent a lot of time talking to our law enforcement, and one of the problems of course is you don't have to stick a gun to somebody's head to steal their money now; you can just take their identity and steal their money. Because a gun is not used, frequently this crime sort of goes to the end of the list of everything else you are doing. What is the one thing we need to do in law enforcement that would help you prosecute the crime and what is the solution to this obstacle? Because the perpetrator knows that they are probably not going to be prosecuted; they know they are very good at going across city lines, county lines, State lines; they know how much they have to steal before it becomes a felony.

I have known some local police officers who have arrested the same person over and over and over again and let them go because no one was willing to prosecute. What is the solution? What do we do? Do we need to make the laws tougher, the penalties larger? What do we need to do? And if each panel member would answer that question, I would appreciate it.

Mr. BEALES. I think one thing that would clearly help is the penalty enhancement legislation that I know has been introduced in the Senate and I believe has been introduced in the House as well. I think prosecutors look to the length of time that they can get by alleging a particular offense. I think that longer penalties and the change in the structure of penalties to make it more like the gun laws where there is an add-on if you steal an identity in committing another crime, it is an additional sentence added on to whatever sentence there is for the base offense. I think those are approaches that can make prosecutors more willing to prosecute the cases and then enhance deterrence.

Ms. HOOLEY. Thank you.

Mr. MIHALKO. I think one of the things that would be most beneficial to us is an increase in probably the appropriations for the Justice Department to hire assistant U.S. attorneys to handle these types of prosecutions. What we have seen is that there are different U.S. attorneys offices that have different thresholds before they are going to accept identity theft cases for prosecution. It may be $70,000; it may be $100,000, which makes it less attractive to bring those cases because they are not going to be prosecuted. There are a lot of law enforcement resources devoted on the Federal, State and local level to investigating identity theft crimes.

Ms. HOOLEY. Okay, thank you.

Mr. CADDIGAN. I think we are on an upswing with regard to the enforcement and the prosecution. We have seen some enhancements. We have seen some legislative benefits recently. I also think we have seen a shift in the prioritization of these type of crimes in our U.S. attorneys's and district attorneys's offices. I have also seen where we have a better sharing relationship between the State and the Federal with regard to where the biggest bang, if you will, will come for prosecution, depending upon the magnitude, the loss and all the other factors that go into determining prosecution.

So the enhancements that I think we have seen are starting to take effect and hopefully we will see that continue in the future.

Ms. HOOLEY. Thank you.

Ms. VIVERETTE. Yes, ma'am, having identity theft as a specific crime has been helpful. Prior to having that in our State, it was underreported because it was reported as a theft and not identity crime.

Ms. HOOLEY. Okay.

Ms. VIVERETTE. Enhance penalties I think would be important and also the addition of resources for officers to follow up on a crime. Right now, they often have the information, but they do not have the investigative resources to go out and make the arrest.

Ms. HOOLEY. Thank you very much.

Chairman BACHUS. Thank you.

Ms. Capito?

Mrs. CAPITO. Yes, I have just two brief questions. For Mr. Caddigan, you testified that the method of identity theft that may be most difficult to prevent is theft by a collusive employee. What are some possible ways to combat such theft? And also in line with that, that many of the identity criminals use information obtained from companies or off of Web sites, and what can companies do to prevent such intrusions?

Mr. CADDIGAN. The insider threat industry will tell you it is their number one concern, protecting not only their database, but their systems. Again, we believe in prevention; we believe in education. An initiative that we began about two years ago, not quite two years ago now, is an insider threat study. What it basically does is reach out starting with our investigative cases that involve such type of activity. They reach back out to the businesses and ask them to provide a little bit more information as to the prevention methods they use, the safeguards they use, and actually provide advice on how they can better themselves in that arena. That initiative is ongoing. It has reached across the country.

We already see some impact with regard to information sharing within sectors, business sectors. We think that because not only the identity theft portion of criminal activity to the insider, proprietary issues, customer-based issues, there is a lot of need for protection in that arena. Again, not overnight, but I think the right steps are being taken to provide an awareness and also to give viable solutions in a security-minded atmosphere on how you can better safeguard your material as a small, medium and large business. Those initiatives are ongoing.

Mrs. CAPITO. Thank you. I just have one additional question, and this is for anybody who thinks they have an idea. I am curious to know the demographics of someone who could fall prey to identity theft. Is it someone who has the information on the Internet? Is it the elderly? Is it someone in big cities? Is it everywhere? Has it been categorized to a point? I am just curious to know what kind of statistics have been gathered, understanding that identity theft has just now been identified as a crime, or at least one that has been reported.

Mr. Beales?

Mr. BEALES. In our complaint database, the victims look pretty much like the population at large. There are not very many children, but other than that, it pretty much mirrors the distribution of the population. There is no one group that is disproportionately affected. We have completed a random sample survey of identity

theft that we hope to release within the next few weeks that will give us a more comprehensive picture of the level of identity theft and also of the nature of who is victimized, but what we see in our complaint data is it just looks like the population at large.

Mrs. CAPITO. Any other comments?

Mr. CADDIGAN. From the enforcement perspective, we rely on the FTC data and we find it to be consistent with our casework. The vulnerabilities are again from the simple trash theft to you dealt with a business on the Internet that was the unfortunate victim of a hacking. It funs the full gamut. No one is particularly targeted.

Mrs. CAPITO. What would be the average time that someone would realize that their identity has been stolen? Would I find out in a month, in a week?

Mr. BEALES. In our complaint data, 48 percent find it out within a month, and an additional number find it out within 1 to 6 months. Within a year, it is 78 percent find it out within a year.

Mrs. CAPITO. I have no further questions. Thank you.

Chairman BACHUS. My first question may be just to follow on that, Mr. Beales, the postal agent testified that it was an average of 14 months to discover?

Mr. MIHALKO. Right. It is about 14 months according to our data before it is discovered, before a victim discovers that they have been a victim of identity theft.

Chairman BACHUS. I am not sure how we square that with Mr. Beales's testimony just moments ago. Are there a significant number that are taking 12 to 14 months to discover, Mr. Beales? What about Mr. Mihalko's testimony?

Mr. BEALES. There certainly are some that take that long, and I don't know the statistical basis for that. What we see in our complaints, and it is just our complaints, is what I reported. Now, I just don't know, in terms of what, it is about 7 percent that take between one and two years and another 8 percent that take between 2 and 4 years to discover it, and then there is a tail of about 5 percent where it takes more than 5 years before it is discovered. So there are some cases that are out there in terms of it taking a long time, but most people find out quickly in our complaint data.

Chairman BACHUS. Okay. I will end the questioning with this question to you, Mr. Beales. FTC Chairman Muris has testified that you are considering different proposals to combat identity theft. You testified at this hearing and previous hearings that you are working on proposals to combat it or additional proposals. This committee anticipates marking up FTC reauthorization next month, at least that is what is anticipated at this time. Will the FTC have any formal proposals to make to this committee that can be incorporated in legislation this month?

Mr. BEALES. We would hope to not be too late, and whether we are too late or not, we are of course willing to offer whatever technical assistance we can in your effort.

Chairman BACHUS. It would be extremely helpful if the Federal agency that is charged with oversight and investigation and coming up with remedies could offer us some formal proposals prior to reauthorization.

Mr. BEALES. We understand that and we will do our best.

Chairman BACHUS. Thank you.

This concludes the testimony of the first panel. The first panel is discharged and we will go immediately to consideration of the second panel. I appreciate your testimony and you are discharged.

The second panel is made up of two victims of identity theft. While they are making their way to the witness table, I might simply say that whether you go by the FTC testimony of basically 125,000 victims of identity theft each year, or you go by the Justice Department records which indicate as many as 500,000 victims of identity theft, we do know that those are both significant numbers. We know that as many as 500,000 reported cases and we know that for each of those cases there is an emotional and financial toll on the victims.

In this second panel, we will actually hear from two of these victims, which in the one regard will be representing a much larger group of millions of American citizens each year who find themselves the victims of identity fraud. I want to welcome our second panel. Our two witnesses, Ms. Maureen Mitchell of Madison, Ohio, formerly of Queens, New York, is that right?

Ms. MITCHELL. That is correct, Mr. Chairman.

Chairman BACHUS. That is correct, thank you. And also Commander Frank Mellott, a U.S. Navy victim of identity theft. You are also here testifying on behalf of the Identity Theft Resource Center.

Commander MELLOTT. Yes, sir, I am, but principally on my own.

Chairman BACHUS. Would you tell this committee what actually the Identity Theft Resource Center is?

Commander MELLOTT. The Identity Theft Resource Center is a victim advocacy group and counseling assistance for victims of identity theft. I am the military assistance coordinator and also the mid-Atlantic-Virginia area regional coordinator. I see primarily cases that involve active-duty, retired or reserve members who are dealing with some of the unique aspects when a military member is a victim.

Chairman BACHUS. I think Mr. Sanders testified that it is a horrendous crime, but it is particularly deplorable or despicable when the victims of identity theft are members of the military serving overseas in defense of our country. It is totally reprehensible that someone would do such a thing to our men and women in uniform. So we welcome your testimony here today.

Also, Ms. Mitchell, I have read your testimony and it has truly been a nightmare for you, just almost inconceivable that someone has to go through what you have gone through. At this time, if you will lead off the testimony.

STATEMENT OF MAUREEN V. MITCHELL, MADISON, OH, VICTIM OF IDENTITY THEFT

Ms. MITCHELL. Thank you, Mr. Chairman.

It is a pleasure and a privilege to be here and I want to express particular appreciation to Congressman LaTourette and Congresswoman Hooley for their efforts and the committee's efforts. And I wanted to say just a personal hello to Congressman Crowley. Joe Crowley and I grew up together in Woodside, New York.

We have been the victims of identity theft and we were not only victims once, we were victims twice. We are a typical middle-class

family. We do not have extraordinary assets and we had always taken the normal consumer protections that we are all advised to take to safeguard our information. We shred our outgoing trash. We were never robbed. We were never burglarized. We never lost our credit cards, and we had checked our credit report in March of 1999 to ensure its accuracy.

Yet in September of 1999, we received a phone call from our KeyBank MasterCard service provider questioning an unusual pattern of activity on our credit card. We were very fortunate that they noticed that unusual level of activity. It turns out that that was the start of our identity theft nightmare when we learned that fraudulent purchases had been made, mail-order purchases by criminals who did not have our credit cards in their possession because we had not lost ours, but they had obtained our credit card number. We do not throw out our credit card receipts intact. And in the days when we all had carbons on our credit cards, when we used them, we obtained the carbons and used to rip them up. We are extremely conscientious about safeguarding our information.

We did not bank on the Internet. We did not order merchandise via the Internet. We did not use an Internet program to balance our checkbook. And we found ourselves victims of this. Unfortunately for us in September of 1999 when our MasterCard account number was compromised, our bank closed our credit card account number and told us we would not be responsible for the fraudulent charges. However, they did not suggest that we put fraud alerts on our credit reports, and they left making out a police report to our option. I did make out a police report because if was a few thousand dollars worth of charges that were made using our credit.

In November 1999, 2 months later, we received a phone call from a J.C. Penney credit representative from New Mexico. We have been residents of Ohio since 1978, finding out that criminals in Illinois, and it was in Illinois that the fraudulent mail order charges were made also, had used my husband's name and Social Security number to obtain a line of credit at the J.C. Penney store in Illinois. It was the J.C. Penney's representative who suggested we put fraud alerts on our credit reports, which I did immediately on November 15.

When I contacted Trans Union, Experian and Equifax, the three major reporting bureaus, I was dismayed to learn that there had been over 25 inquiries into our credit during that 2-month period of time between the initial credit card account number being compromised and the phone call from J.C. Penney's, and criminals had changed our address six times. I did place the fraud alerts on our credit report and I also put 7-year consumer statements, and it took me over 400 hours of time to dispute 30 fraudulent accounts that criminals had opened in our names out of State. There had not been 30 inquiries into our credit in the entire 20 some-odd years my husband and I had been married at that point, yet 30 inquiries into our credit in a 2-month period of time did not send up red flags to anybody at the credit reporting agencies. I think that needs to be addressed.

Four hundred hours, hundreds and hundreds of pages of documentation were required by us. I found the information from the Federal Trade Commission's identity theft clearinghouse to be

helpful to me. Kathleen Lund from the Federal Trade Commission was the identity theft counselor whom I had spoken to, and she did offer me some guidance and assistance and some emotional support. I also put that in the testimony, because as a victim of identity theft, your life is spinning out of control and we never were able to ascertain our point of compromise. I did meet with our Congressman Steve LaTourette, and it was through his intervention that we were able to be in touch with the FBI. We ultimately wound up with the United States Secret Service, the United States Postal Inspectors, the Office of the Inspector General of the Social Security Administration, and the FBI, plus our local police department as the investigating authorities.

Criminals in Illinois did a $150,000 worth of new credit applications in our names. We had previously had an impeccable credit report. Our FICO scores were in the low 800s; $150,000; 30 different accounts. They bought a Ford Expedition. They bought a Lincoln Navigator. Neither of those vehicles were sitting in my driveway. And two months after the criminals purchased the Ford Expedition, they torched that vehicle, filed a fraudulent insurance claim in my husband's name, and then we had to deal with the National Insurance Crime Fraud Bureau because there was a fraudulent insurance claim filed.

We did get good cooperation from our local police department in Madison, Ohio. As a matter of fact, my husband and I and both of our adult children are carrying a notarized letter from our police chief in our wallets at all times saying that we are the victims of these crimes and not the criminals, because if we get pulled over for some innocuous traffic violation, we can find out that there are warrants under our Social Security numbers that we know nothing of.

Two years after the criminals initially victimized us, and it was 2 years of fighting our way, it is a task made for Hercules that requires the wisdom of Solomon, as a victim of identity theft, to fight your way through the system. Two years afterwards, with the security protocols in place, and I had insisted upon security protocols on our bank accounts, we were making a purchase of a small home for both of our adult children who are students to live in while they were attending medical school and college. The fraudulent purchase of the Ford Expedition, the one that the criminals torched and filed the fraudulent claim on, showed up on my husband's credit report as we applied for the mortgage, lowered my husband's FICO credit score by 118 points, and we were almost denied the loan for the mortgage that we were legitimately applying for.

My girlfriend Cathy said to me, "You know, Maureen, you just should have had the criminals apply for the mortgage. They would have gotten it with no problem." And there may be some truth to that statement. We again had that remedied. This account had bounced back onto my husband's credit report. They knew it was a fraudulent account, yet it reappeared.

In October of 2001, we received at home a very alarming phone call from an intercity branch of our bank asking whether we were having trouble with our bank accounts. I had placed security protocols on our bank accounts. I had insisted upon them. Photo ID and password, and the password was not mother's maiden name or any-

thing else that would be available on a genealogical Web site. Photo ID and password required on our bank accounts, and our local branch of KeyBank, and they have known us for 20 years, insisted that we use those protocols every time we banked, and we insisted upon it also. Yet when I received this phone call on October 30, criminals had made four fraudulent withdrawals from our personal bank accounts. It was upon the attempt of the fifth fraudulent withdrawal that we were finally notified. Criminals removed $34,006.50 from our bank accounts in spite of the fact that photo ID and password was required on these accounts.

We had an arrest made in the State of Illinois, Lansing, Illinois as a matter of fact. The criminal there was prosecuted. He was sentenced to three years in the Illinois Department of Corrections in 1999 when he was arrested. He served less than a year. We currently have a case pending in Cuyahoga County, Ohio. The criminal who made the KeyBank fraudulent withdrawals a week after I received the phone call was attempting to make a $5,000 credit application using my name at the Circuit City store in North Randall, Ohio. When the Illinois crimes were occurring, there were criminals impostoring my husband. When the Ohio crimes were occurring, there were criminals impostoring me.

She was eventually apprehended at the Circuit City store because the fraud alerts on our credit reports did indeed work. Why the security protocols on our bank accounts did not work still remains to be answered. One of the hardest things in being a victim of identity theft is that you are repeatedly subject to having your integrity and character questioned. You are perceived as the criminal and the scales of justice are tipped in the wrong direction in this regard. The criminal is assumed innocent until proven guilty, but the victim of identity theft is assumed guilty until you prove your innocence.

We started to receive phone calls from collection specialists at our home, wanting to know why we were late for the payments on our Lincoln Navigator and our Ford Expedition, the vehicles that we had not purchased. It amazed me that the collection specialist could find the real Ray and Maureen Mitchell when they wanted their money. Too bad nobody bothered to find the real Ray and Maureen Mitchell before they loaned out that money. There are protocols that should work when they are in place. No system is perfect. Our protocols should not have failed. They did. We had to re-work our way through the system. And when the criminal impostor of me was arrested at Circuit City in North Randall, Ohio, she was found to have an Ohio DMV-issued photo identification card that contained her picture but all of my information.

And when that criminal had obtained that photo ID card, my driver's license was automatically suspended in the State of Ohio because it is illegal to have a driver's license and a State-issued photo ID card. So as a result of that impostor's activities, our bank accounts were frozen on October 30, 2001 and I had a suspended driver's license. I am a registered nurse. I am a licensed realtor. We are entitled to have access to our own monies and we are entitled to safeguard our personal licenses. I was scared to death that my real estate or my nursing license would be impacted by criminals because they had already impacted my driver's license.

Our lives were turned upside down for 4 years because of identity theft, and the only risk factor that we had of becoming victims of this crime was that we had an impeccably good credit report. The demographics, as we heard in previous testimony, will show that this crime does affect all people. But if you do not have creditworthiness, you are not sought out as a victim because it does not serve the purpose of the criminals.

Words cannot begin to describe what this has been like for us. We have fought our way through this tooth and nail. We have received help from Congressman LaTourette. I had the privilege of testifying in a Senate subcommittee at the request of Senator Kyl. We have received help from the Federal Trade Commission. This is a national epidemic and it has to be stopped. Billions of dollars a year are being lost because of identity theft crimes and credit fraud. The impact that it has on victims' lives is unbelievable. Your credit score does not only reflect your loan worthiness. It also reflects to many entities, insurance industries, employers, et cetera, they equate that number with your good character. To have criminals assail that is unacceptable and incomprehensible.

I would encourage all of you to please read my full written testimony. I do realize it is lengthy. Believe me, I compressed four years of details into those pages. I will be happy to answer any questions and I again thank you for the privilege of having testified.

[The prepared statement of Maureen V. Mitchell can be found on page 177 in the appendix.]

Chairman BACHUS. Thank you, Ms. Mitchell.

Commander Mellott?

STATEMENT OF COMMANDER FRANK MELLOTT, UNITED STATES NAVY, VICTIM OF IDENTITY THEFT, ON BEHALF OF THE IDENTITY THEFT RESOURCE CENTER

Commander MELLOTT. Yes, sir, Mr. Chairman, Ranking Member and other members of the committee, thank you very much for the opportunity to testify today. The views and opinions I express today are my own and do not necessarily represent the Department of Defense or the Navy.

I am here because I am a victim of identity theft, but I am also here because I am a victim of what I would call a blunder by the credit reporting industry. My ordeal began back in the summer of 2001 when my wife walked in from the mailbox carrying a letter from the Department of Treasury. That letter said that my $5,000 tax refund, along with all Federal payments, was diverted to California to pay back child support. Now, my paycheck is a Federal payment so I was a little concerned that in less than two weeks I had zero income.

However, the more I thought about it, I became even more concerned with the long-term consequences. As a military member, particularly as an officer working in the field in which I do, a security clearance is an essential component to my ability to function. My security clearance can be affected almost instantly by my credit history. If I lose my security clearance, I am unable to do my job. I am unable to compete with peers for promotion. I am unable to compete for milestone positions such as command of a unit or a

squadron, and fundamentally it affects my ability to support my family in my chosen vocation, service to the country.

This all began in calendar year 2000 when my half-brother used my Social Security number and only my Social Security number on W-2 forms he filed with the Breckenridge Group and with Pep Boys in California. Now, I cannot say whether either of those companies verified identity documents when they hired him, but I would suspect that they did not.

In the end, California found out that he was working again by name, and since he owed about $75,000 in back child support, they sent his data off to the Federal agencies for collection. Unfortunately, the data they pulled was the data he supplied, my Social Security number, and the next thing you know I got the letter.

So unfortunately, I am staring this letter in the face. Instead of spending a summer leave period enjoying some time catching up with my two sons after nearly six years of straight sea duty, I am spending it fighting jurisdictional issues. I have got three police agencies all going like this when I tried to file a police report. I am spending hours and hours either writing letters or on the phones with credit reporting agencies trying to track the source of these problems and then get them resolved. I am trying to keep my security clearance folks flooded with information so that I do not lose my security clearance, because quite honestly it is much easier to take one away than it is to get it restored. Once it is gone, it is very difficult.

Of course, I am working with the IRS to try and resolve about $10,000 of income that was reported against my Social Security number that I did not claim. Unfortunately, in February 2002 the problems continued. I had already started the cleanup effort so I had placed fraud alerts with the three credit reporting agencies. Unfortunately, my brother was still able to go out and get cellular phone service with AT&T Wireless in spite of those alerts, but that was not the end of it. The worst happened when Experian merged my credit file with that of the criminal, my brother's. So now instead of having one or two bad entries in my credit file from which I am trying to correct, I now have 30 or more. I have incorrect addresses, incorrect employers. I have two aliases. I have alternate uses of my Social Security number, a host of collection actions, even listing his wife as mine. Any single one of those could have had a severe and adverse affect on my ability to function as a naval officer by removing my security clearance.

I found the credit industry is unfortunately not quite as responsive as I would hope. As a military member with frequent moves I was very concerned about having specific language put in the fraud alert. So I sent all three of them a certified return receipt letter asking them to incorporate specific language. Not a single one of them incorporated that language. Not a single one of them even bothered to reply.

Now, as bad as this sounds for me that the identity theft tarnished my image, the blunder by the industry could have done the same thing. Although my case has been largely resolved, as an officer responsible for the welfare of my troops I am very concerned about how this affects the 19-year-old soldiers, sailors, airmen, Coast Guardsmen and Marines serving around the world right

now. This problem is virtually impossible to clear up unless you are right there. It is hard enough right here fighting the jurisdictional issues military members face when oftentimes three or more States are involved.

But fundamentally, our nation is at war and our military members can be deployed anywhere in the world at a moment's notice. We have heard this morning that it can take months for people to find out they are victims of a crime or a mistake and we have heard how it can take a substantially longer period of time to correct that. How do we expect that young soldier to be doing that from the streets of Baghdad at night? How do we expect him to spend that 175 hours or the $1,400 in estimated out-of-pocket costs to correct problems or mistakes?

I encourage this committee to take any action they can to improve accountability. Obviously, I have some opinions. I think there needs to be some increased accountability for the accuracy of data. I think there needs to be some specific measures targeted to protect military members on active duty. I think the committee needs to take a good look at some of the critical nodes in the credit reporting and credit-issuing arena.

I do have to thank Congresswoman Loretta Sanchez for her efforts to assist me in my case, as well as specific thanks to Special Agent Chris Behe of the Navy Criminal Investigative Service who was the first officer to take a police report which subsequently opened doors and led to a prosecution.

Sir, I have completed my statement and I stand by to answer any questions you may have.

[The prepared statement of Frank Mellot can be found on page 161 in the appendix.]

Chairman BACHUS. Commander, did your brother ever go to jail? Was he ever prosecuted?

Commander MELLOTT. Yes, sir. The Navy criminal investigative report I was able to forward to California and then they were able to take action on it. They arrested him. Unfortunately, he had been arrested and appeared in court once before I was even notified, and found out that his final hearing was going to take place the next morning, so I spent the better part of a day putting together a victim impact statement. He was awarded a 3-year suspended sentence on two felony counts for falsely providing information on the W-2 forms. He spent 120 days in jail and he is out on supervised probation.

Chairman BACHUS. Has he stopped doing it?

Commander MELLOTT. At this point, he has, although, sir, I continue to see lingering effects from it. About 4 or 5 months ago I got a letter addressed to his wife at my address about a $5,000 bill that was outstanding.

Chairman BACHUS. You have never not been to California during this period of time, is that right?

Commander MELLOTT. I can't say for sure during the period. I most certainly visited at least once. I am a legal resident of California, but I was stationed in the State of Washington and then in Rhode Island before being transferred to Virginia where I am at now.

Chairman BACHUS. So after you reported what was going on and then you would get your credit reports, there was nothing on those credit reports to indicate that there was a problem, right?

Commander MELLOTT. When the initial letter came from Department of Treasury, by the end of the week I was able to establish that it legitimately was not me they were looking for. About a week later, I got the credit reports and then what I found on those credit reports was that it had started much earlier. He had applied for cable TV service in the State of New York with Time-Warner Cable. When he defaulted on the bill, it was reported as a collection action against me. At that point, that was the only thing that showed up on my credit report. It was not until the merging of the two files by, as Experian said, the computer did it, that I encountered a substantial problem with inaccuracies.

Chairman BACHUS. When you wrote to the credit reporting agencies and you said, "here is what is going on," subsequent to that, did you obtain your credit report? You said that none of them listed this information?

Commander MELLOTT. I would have to look back in my records, sir, to make sure I quote the exact company that had it. Of the three credit reporting agencies, there was only one that reflected the outstanding Time-Warner bill. Subsequent to that was when the data files were merged. That is when the information in those files in my credit report was substantially incorrect. It has been months trying to get that cleared up.

Chairman BACHUS. Yes, but I am not sure you are following.

Commander MELLOTT. Yes, sir?

Chairman BACHUS. When you wrote to the three credit reporting agencies and you said, "my brother is engaged in this activity, this is the problem," what I am saying is subsequent to that, you said they refused to take any action?

Commander MELLOTT. Yes, sir.

Chairman BACHUS. They did not put your letter in the credit report, or there is no mechanism?

Commander MELLOTT. What I did, sir, was I was concerned because as a military member I move fairly frequently. It is often difficult for credit agencies to keep the information current because I move so often. So what I wanted to do was to try and find a way to, much like Mrs. Mitchell here, provide a much more secure method before somebody issues credit to someone who may be trying to do it in my name.

Chairman BACHUS. Right.

Commander MELLOTT. So I sent a letter that was substantially the same letter to all three asking them to include specific language on the fraud alert. What I wanted somebody to do was that if anybody tried to apply for credit in my name, that they had to cite a photocopy at a minimum, but certainly a military identification card, for a couple of reasons. One, that assists me with jurisdictional issues if it happens, because now it is impersonating an active duty member, but also it is a photo ID that has the information on it. Not a single one of them did that. They did not put that language into the permanent fraud alert. They put their standard language on, which of course refers them to the phone number and address that I have on record that, well I am sorry, three moves

in a year make it very difficult for that to keep up. I recognized that the standard alert was not going to suit the bill, asked them to put something specific on, and they ignored it.

Chairman BACHUS. Okay. Thank you.

Mr. LaTourette?

Mr. LATOURETTE. Thank you, Mr. Chairman.

Both of you talked about jurisdictional things, and I can remember, Maureen, when you were dealing with the criminals in Illinois, I used to be a county prosecutor and I tend to think that States should principally deal with criminal matters and only in extraordinary circumstances call for the Federalization of crimes. But it was my recollection that what was described by the first panel was existence in the different jurisdictions and they had different thresholds. I don't remember if it was $50,000 or $100,000, but they said they were really not going to take a look at your case at the Federal level unless you reach $100,000. As a result in Illinois, if I remember correctly, they were treated with what in Ohio would be fourth degree felonies that carry maybe a year and a half in prison, and typically are probationable offenses where people get out.

So I think both of your stories are reasons why the majority of the members of this committee have become convinced that this is a national problem that needs to be addressed nationally and can't be left to the devices or the different States, for the reason in your case, well in both of your cases, you lived in one State and the crimes were taking place in different States.

Maureen, I again want to thank you for coming. You came on your own dime from Ohio and I appreciate that. I would think that, and I know, sort of like a softball question, I know that your experience has probably given you the ability and the time to think up a long list of suggestions that the government could do to help people that find themselves in the same position as you and Ray found yourselves in. Would you want to share a few of those with us?

Ms. MITCHELL. Thank you, Congressman LaTourette. Yes, I would.

I cannot stress enough to the committee that we had zero risk factors of this happening to us. However, that is not the case for most consumers. So the truncation of the credit card numbers on credit card receipts is indeed important. I recently saw a receipt for a Discover card purchase that our daughter had made using her account. It not only contained her Discover card account number, it also contained her name. If that receipt were inadvertently placed in the trash and a criminal were to obtain it, they would have all of the information that they needed from one careless disposal of a credit card receipt to start committing crimes.

I do think that there needs to be a free annual consumer credit report available to any consumer that requests it. We had looked at our consumer credit reports in March of 1999. It was a fluke that we did that because we were putting a mortgage on a property, so I had the lender send me a copy of it. If I were not putting a mortgage on a property, I would never have requested that. An annual review of the credit reports by the consumer is good for two different reasons. One, many victims of identity theft are often unaware that they are victims and may be unaware of it for years

until the next time they apply for credit. Consumer credit reports are also, if you are unfamiliar with reading them, somewhat of a challenge to decipher at first. So it would also give the American consumer an opportunity to familiarize themselves with the verbiage in the consumer credit report so that as they familiarize themselves with it, they would more easily recognize in the future if something were indeed wrong. So those would be two things that I would strongly suggest.

Mr. LATOURETTE. I think that, and some of those point to the need to hand over the credit report, but some of those things put the burden on the customer, the consumer. The legislation that Mrs. Hooley and I have worked up also shifts the burden to those who extend credit a little bit. It seems to me that most of us here, you are not only a nurse, but you are a realtor, most of us and most of the people of our acquaintance probably do not move six or seven times within the course of a year. It seems to me that those who are in a position to extend credit, and come across a credit file where there are people moving from Ohio to California to Illinois and to Texas during a 12-or an 18-month period, perhaps a burden should be placed upon them as well to say maybe this is something that is not quite right. I would assume that is something that you would think would be a good idea as well.

Ms. MITCHELL. I absolutely agree with you, Congressman. Anything that does not match the consumer record of file on the credit report when a new application of credit is filed should serve as a red flag, not requiring necessarily denial of credit, but requiring further investigation into the legitimacy of that application before credit is indeed granted. We have resided at the same address for well over 20 years. Yet as a result of criminals in Illinois, and we were victimized by an organized identity theft ring, as a result of the criminals in Illinois we now showed six address changes on our credit reports within a two-month period of time. We had lived at the same address stable for 20 years. We did not hopscotch from house to house six times in 2 months in Illinois.

Mr. LATOURETTE. Right. I think when we were talking a couple of years ago, the notion, and to the commander, you as well with the experience with your half-brother, there is a thought that the prison sentences for people convicted of this crime ought to be enhanced and increased from again typically based upon the amount of money that is stolen, and if you are in a variety of different jurisdictions you can steal a little bit of money here, a little bit of money there, and in the aggregate it turns out to be a lot, but under the State penal code it may affect the classification of crime. So commander first with you, would you like to see legislation that increased the available penalties for people who engage in this activity?

Commander MELLOTT. Sir, absolutely. To Mrs. Mitchell's recommendations and personally, I would also like to see a mandatory observation of fraud alerts. I think if companies were held accountable for not observing a fraud alert that was on an account, then they would be a lot more careful about issuing credit to people who quite honestly are doing it fraudulently.

Mr. LATOURETTE. And Maureen, is that something you wish we would consider as well, that is the increased criminal penalties, lock them up longer?

Ms. MITCHELL. Absolutely. The criminal who was prosecuted in the State of Illinois, who was apprehended impostoring my husband, was eventually sentenced to 3 years in the Illinois Department of Correction. He would have received probation, in my opinion, had we not been assertive consumers willing to prosecute and had not Congressman LaTourette's office intervened in that. The damages that were done to us were extensive. He was one of many, but if these criminals are able to commit these crimes and count on probation instead of incarceration, we are not offering any deterrent for these crimes to continue. They need to be held accountable.

I would like to add, too, that some of the merchants also need to be held accountable. When the criminals purchased the Ford Expedition in my husband's name, there were six glaringly obvious errors on that credit application. Our name was even misspelled. They put down 3-0-0 as the area code to verify their place of employment. You don't really need to be an Einstein to know that 3-0-0 is not a valid area code in the continental United States. Yet they received approval for a $40,000 purchase on a vehicle. The merchants need to be held accountable. Good business practices, common sense and due diligence need to be used at all steps of the lending process to ensure that the monies are indeed being loaned to the real individual.

Mr. LATOURETTE. Thank you very much.

Thank you, Mr. Chairman.

Chairman BACHUS. Thank you.

We have no further questions for Ms. Mitchell or Mr. Mellott.

Ms. Mitchell, one thing, you said they misspelled your name?

Ms. MITCHELL. Yes, they did.

Chairman BACHUS. Is that the name "Mitchell" you mean?

Ms. MITCHELL. Yes, they did.

Chairman BACHUS. Okay.

Ms. MITCHELL. Yes, they did. And it was not only misspelled on the application filed by the criminal, it was also misspelled on the facts from the lender granting the car dealership the loan approval. The only thing that matched us on that application was my husband's Social Security number. The Social Security number and the State driver's licenses have become the de facto form of identification in the United States. Safeguards need to be in place to ensure that those numbers safeguard the real individuals from having their identities compromised.

Chairman BACHUS. Thank you.

Have you put a financial cost estimate on what this cost you?

Ms. MITCHELL. I can tell you that the criminals fraudulently applied for $150,000 worth of lines of credit in 1999 in the Illinois area in our names. In 2001, they removed $34,000 from our bank accounts. Those monies were eventually restored with interest. We had our bank accounts frozen. It was extraordinarily embarrassing. Out-of-pocket financial expenses for us are in the $2,000 to $3,000 price range, the nearest estimates that I could give. It is countless hours lost in time, sleepless nights, and sprouting gray hairs. The blood, sweat and tears that went into trying to resolve our identity

theft victimization, it is indescribable to try and put that into words. But it was a few thousand dollars out of pocket expense and over 500 hours of time, very dedicated time, and hundreds of pages of documentation.

Fortunately now, and I think it was a direct result of a Senate subcommittee testimony that Senator Kyl chaired, the FTC now does have the uniform victim reporting identity theft affidavit, so future identity theft victims will not have reams of paperwork, because our experience was that the individual merchants all required individual protocols. That is no longer the case. It is still a daunting task for the victim of identity theft to try and have their credit restored, and I am not sure that it is ever restored fully.

Chairman BACHUS. Thank you.

Commander, do you have any last remarks?

Commander MELLOTT. No, sir. Thank you for inviting me. Anything I can do to help, I am standing by.

Chairman BACHUS. Thank you. We appreciate your assistance to the committee and your testimony in sharing your experiences. We appreciate your testimony.

At this time, you all are discharged and we will request that our third panel make their way to the witness table.

Mr. TIBERI. [Presiding.] I thank the panelists from our third panel for being here today. I will quickly introduce the panel, and then we can begin.

Starting from my far left, Ms. Amy Hanson, President of the FACS Group, a subsidiary of Federated Department Stores; Mr. Jim Kallstrom, Senior Executive Vice President, MBNA America Bank; Joshua Peirez, Senior Vice President and Assistant General Counsel, MasterCard International; Ms. Janell Mayo Duncan, Legislative and Regulatory Counsel, Consumers Union; Mr. Joseph Ansanelli, CEO of Vontu; and last but not least, Mr. Lee Lundy, Vice President, Consumer Services, Experian.

Good. Thank you all for coming. We will begin with Ms. Hanson. I remind everybody that you will see a clock that will eventually turn red in five minutes. At that point, if you could sum up your remarks and you will be able to submit your written testimony as well.

Ms. Hanson, the floor is yours.

STATEMENT OF AMY HANSON, PRESIDENT, FINANCIAL, ADMINISTRATIVE CREDIT SERVICES, INC., (FACS GROUP) ON BEHALF OF THE NATIONAL RETAIL FEDERATION

Ms. HANSON. Thank you. Good afternoon. My name is Amy Hanson. I am President of the FACS Group, which provides credit and other administrative services for Federated Department Stores and its affiliated bank. I am testifying today on behalf of the National Retail Federation.

I would like to thank Chairman Bachus for providing me with the opportunity to testify before the House Financial Institutions Subcommittee about the growing problem of identity theft and the steps that Federated is taking to protect our customers and reduce losses from these crimes.

By way of background, Federated is comprised of seven merchant nameplates, Macy's, Bloomingdale's, Burdine's, Rich's, Lazarus,

Goldsmith's and the Bon Marche. We issue our proprietary credit cards under these names through our affiliated bank. In fiscal year 2000, Federated reached a peak for identity theft-related losses with 5,678 cases representing a total expense of just under $8 million. In the past two years, we have experienced a decline of approximately 33 percent in the number of identity theft cases and recognized a $3.2 million reduction in expense. In the last six months, we have seen a 41 percent improvement in ID theft cases compared to last year. We feel strongly we are making progress in our efforts to protect our customers due to our ability to optimize technology and information, both of which are critical in this fight.

Identity theft can occur in two basic ways in our stores: through an application for a proprietary account or through a takeover of an existing credit card account. Over the last several years, we have continued to add additional verification steps to our internal processes to prevent identity theft. This issue is of paramount importance to us because after all, these are our customers who expect both a high level of personalized service and personal security in our stores.

Instant credit represents about 93 percent of all new accounts opened by customers at Federated. This process takes place at point of sale and relies on a highly automated and relatively quick procedure to verify an applicant's ID and check their credit report. In order to cut down on fraud, we have implemented many processes to protect our customers. These include validating applicant information against credit reports, checking applicant data against our internal fraud file, and checking the consumer credit bureau report for fraud alerts placed there by the customer. If there are discrepancies in any of the application information, the application is declined.

Our screening does not stop there. We have a process by which customer charges are reviewed for out-of-pattern behavior, high velocity purchasing, making payments on their account for significantly more than their balance due, and high-risk merchandise purchases. We also systemically prevent the mailing of a new credit card on a recently changed address.

In addition, our fraud prevention group utilizes technology to crosscheck Internet orders and an affiliate fulfillment system to search multiple orders across affiliate chains. This ability proved very helpful in discovering an Internet fraud ring where the perpetrators were placing several orders for the same merchandise on different Federated Web sites, then shipping these items to various addresses in the U.S. They then collected the items for shipment overseas. Fortunately, we were able to uncover and shut down this ring using our affiliate sharing tools.

I would like to be able to say that FACS has prevented all of the fraudulent applications this year, but I can't. Unfortunately, sophisticated identity thieves continue to work diligently to bypass our systems and were successful in 2002 at a rate of 7 per every 10,000 applications processed, less than one-tenth of 1 percent. This in my view is not the result of a flawed system, but the result of determined criminals with sophisticated tools like computers and the Internet. You see, the most identity thieves know how to

produce near-perfect identity documents such as State-issued driver's licenses and counterfeit credit cards.

For these types of criminals, there is very little else we can do to detect and prevent the crime, and retailers, like other businesses, are looking to the States and the Federal government to begin producing the most secure and foolproof identity documents possible. Our ultimate goal is to confirm the identity of the customer and ensure their identity is not compromised.

With identity theft representing such a small fraction of total credit applications, it is often a case of looking for a needle in a haystack. Further, identity thieves thrive on being anonymous and rely on the assumption that a large retailer such as Federated cannot put a name and face together in order to prevent fraud. This is why it is so important for retailers to know our customers, and the only way we can do this is through the use of information. Information flows between FACS and the credit bureaus or between our corporate nameplates. That, combined with sophisticated technology and scoring models, cuts down on fraud and allows us to offer exceptional customer service.

As you know, identity theft is a crime with at least two victims: the individual whose identity was stolen and the businesses that bear the financial cost of the crime. Clearly, it is the individual victim that is the most directly hurt, but if identity theft crimes continue to rise, all consumers will ultimately pay as business losses are passed back to them. As such, it is critical that our access to information and prevention opportunities continue. The identity theft criminals adapt and change quickly and we need that same flexibility.

I appreciate the opportunity to testify here today and I look forward to answering your questions, as well as those of the committee.

Thank you.

[The prepared statement of Amy Hanson can be found on page 117 in the appendix.]

Mr. TIBERI. Thank you, Ms. Hanson.

Just as an aside, one of my first credit cards was a Lazarus credit card.

Ms. HANSON. That is good. I hope it is still in your wallet.

[LAUGHTER]

Mr. TIBERI. Mr. Kallstrom?

STATEMENT OF JIM KALLSTROM, SENIOR EXECUTIVE VICE PRESIDENT, MBNA AMERICA BANK

Mr. KALLSTROM. Good afternoon, Mr. Chairman. Thank you for inviting me here today. I think I can safely speak for the entire industry in complimenting the committee for the thoroughness with which you are examining the issues relating to the reauthorization of the Fair Credit Reporting Act. From our perspective, you have constructed a compelling record from which to legislate and we have high praise for the diligence and dedication of the staff who have brought all of this together.

Regarding identity theft, we are in complete agreement with you and the other members. Identity theft, like other serious crimes, is an attack on our customers, our businesses and on our economy.

While it accounts for only about 4 percent of the fraud we experience, as you have just heard it often exacts a personal cost of time, reputation and frustration that is very hard to measure. Viable solutions likely will involve greater participation by all of us, the credit granting industry, retailers, the credit bureaus, law enforcement, prosecutors, government agencies and consumers. But also recognizing that our collective task is made much more difficult by the rampant availability of false identification documents, which is an epidemic in this country today.

As with many crimes, the cliche "forewarned is forearmed" applies to identity theft as well. Ensuring the availability of key information, both to businesses and potential victims alike, goes a long ways towards prevention and apprehension. As Assistant Secretary Abernathy remarked recently, identity theft is not caused by information; it is caused by a lack of information.

In summarizing my statement for the record, I would like to make four points. First, the interests of our customers and the interests of industry are synonymous. Our business philosophy is, find the right customers and keep them. We want our customers to be able to use our products and use them securely. We want our customers to have confidence that we will help protect them against the ravages of identity theft. When fraud does occur, our customers are not responsible for the fraudulent charges and we provide assistance both to help stop further damage and to help in recovering from the identity theft. But as we have just heard, it is far more difficult to restore the confidence of victims and to relieve the effects of having their identity stolen. We agree with our customers who say, reputations, good will, financial well being and consumer confidence are all put at risk because of identity theft. In the end, it hurts every one of us.

Second, prevention and detection of identity theft is what we do with every application and every transaction, 7 days a week, 365 days a year. We invest millions of dollars preventing and detecting identity theft and other types of fraud. We employ hundreds of people who specialize in fraud detection and prevention, and have a sizeable cadre of people dedicated to ensuring our customers are properly identified. We employ extremely sophisticated neuro-networks and experience-based automated strategies to find and reduce fraud and identity theft, from exploring discrepancies between applicants and credit reports, to scrutinizing hundreds of thousands of daily transactions for anomalies. We fight identity theft from the credit application stage through loan repayment. Our customers are critical participants in this process, but there is no question that the Fair Credit Reporting Act is the foundation of this effort. To be successful, we rely upon the kind of uniform current credit information that FCRA has given us.

The third point I would like to make is setting the record straight on a couple of things, affiliate sharing and prescreening. With affiliate sharing, we are aware of no instance, not one, where affiliate sharing resulted in identity theft. To the contrary, it helps the industry fight identity theft. Our experience with prescreening is similar. Prescreening results in substantially fewer fraud attempts, not more. A study released last week by the Information Policy Institute, the IPI, a copy of which I am submitting with my

statement for the record, confirms that the same holds true for the entire industry. In fact, the study found that industry losses from fraudulent prescreened applications amount to four one-thousandths of 1 percent of total sales volume. Eliminating prescreening would likely result in an increase in identity theft. That is so because prescreened offers reflect only names and addresses, less than is in the telephone book. The prescreening process involves more filtering, not less filtering.

One final point, Assistant Secretary of the Treasury Wayne Abernathy understands the industry, understands the problem, and he and others at Treasury have talked about the need for a comprehensive approach to address the problem of identity theft. We agree that any approach should include enhanced prevention, detection and victim assistance. It should include reauthorization of FCRA because, as Assistant Secretary Abernathy says, to do otherwise creates shadows where identity theft can occur. On the enforcement side, the solution should include stiffer penalties, reflecting the serious and pervasive nature of this crime.

We also agree that any solution should help consumers make more informed decisions about information sharing. This can happen by making privacy notices shorter, simpler and in plain English, and making opt-out procedures easier and uniform so that consumers can more easily exercise control of their personal information in a meaningful way. Everyone agrees it would be of enormous benefit to provide consumers with easily digestible privacy notices that include easy opt-out procedures. In fact in a recent survey, we found that our customers overwhelmingly support a simple food label-like notice as the kind of notice they want, a notice they will actually read, that is easily comprehensible, and which allows busy people an opportunity to participate in information sharing decisions in a more meaningful way. It is simply a good idea that will be of great benefit to consumers.

In the end, legislating more and better tools for law enforcement, consumers and the industry to use to prevent, detect and recovery from identity theft is a consumer issue that will help us all. We applaud your attention to these critical issues and I look forward to any questions you might have.

Thank you very much.

[The prepared statement of Jim Kallstrom can be found on page 125 in the appendix.]

Mr. TIBERI. Thank you, Mr. Kallstrom.

Mr. Peirez?

STATEMENT OF JOSHUA L. PEIREZ, SENIOR VICE PRESIDENT AND ASSISTANT GENERAL COUNSEL, MASTERCARD INTERNATIONAL

Mr. PEIREZ. Good morning, Chairman Bachus, Congressman Sanders, and members of the subcommittee.

My name is Joshua Peirez and I am Senior Vice President and Assistant General Counsel at MasterCard International located in Purchase, New York. MasterCard is a global organization comprised of financial institutions that are licensed to use the MasterCard marks. I thank the subcommittee for having a hearing

on this critically important issue and for giving me the opportunity to provide information on combating identity theft.

MasterCard takes its obligation to protect MasterCard cardholders against identity theft and other forms of fraud very seriously. In fact, this issue is a top priority for MasterCard and we have a team of experts, including many ex-law enforcement personnel devoted to combating fraud. We are proud of our strong record of working closely and proactively with Federal, State and local law enforcement agencies to apprehend these criminals.

MasterCard believes its success in fighting fraud is perhaps best demonstrated by noting that our fraud rates have continuously declined over time and are at historically low levels. MasterCard recognizes that identity theft and other fraudulent schemes evolve constantly, and we devote substantial resources to staying one step ahead of the criminals. We continually develop new ways to fight fraud and identity theft. For example, MasterCard has instituted a number of protections against unauthorized use of MasterCard payment cards. These include enhanced security features on the card, the risk-finder service, the address verification service, the issuers clearinghouse service, and our proprietary fraud reporting system. In addition, we have voluntarily implemented a zero-liability rule which means that a MasterCard cardholder will generally not be liable for any fraud losses at all.

Although MasterCard has established these consumer and antifraud protections, one of the most important tools in combating identity theft is the availability of accurate, reliable consumer reports. Providing consumer reports is the role of the credit bureaus which gather information from thousands of sources commonly referred to as furnishers. The reliability of consumer reports as an identity theft prevention tool is largely due to the uniform national standards established by the FCRA. If States impose different obligations on furnishers, the amount and quality of information could substantially decrease.

The FCRA also governs two activities that greatly assist financial institutions in fighting identity theft, affiliate sharing and prescreening. Financial institutions rely on the ability to share information among their affiliates in order to detect and prevent identity theft. This happens, for example, when an application does not match existing information about the same consumer held by an affiliate. Additionally, prescreening also results in fewer cases of identity theft and other fraud than when the accounts are acquired through other means. In this regard, prescreening and affiliate sharing are important weapons in the fight against identity theft.

Other provisions in the FCRA are also useful in limiting the damage to identity theft victims. For example, consumers receive notices if they are denied credit based on information in a consumer report. This flags for the consumer that the consumer's report may contain negative information and allows the consumer to follow up and investigate the matter further. If there is information in the credit report that may be the result of identity theft, the consumer can generally require the credit bureau to correct any error within 30 days. In conclusion, MasterCard is committed to working with government, credit bureaus, our members and cardholders to

ensure that we provide the safest financial environment possible. We take our role in fighting identity theft and fraud very seriously and will continue to research and develop technologies and programs to help with that fight. By making the national uniformity under the FCRA permanent, MasterCard will be able to provide better protection against identity theft and fraudulent activities to its cardholders and issuers.

Thank you again for allowing me to appear before you today on this important topic. I am happy to answer any questions you may have.

[The prepared statement of Joshua L. Peirez can be found on page 195 in the appendix.]

Mr. TIBERI. Thank you, Mr. Peirez.

I am going to yield just a minute to the chairman of the subcommittee.

Chairman BACHUS. I thank you, Mr. Tiberi.

I wanted to take this time to say to Mr. Kallstrom and Mr. Peirez, Mr. Kallstrom from MBNA America and Mr. Peirez from MasterCard, the staffs of your institutions have been very helpful to us in the committee in reviewing legislation on reauthorization for FCRA. They have been very timely in getting back with us and just fully cooperative, and I want to commend both you gentlemen for that. It has been a very good experience for us. I think that the legislation going forward will reflect your expertise. As you say, Mr. Kallstrom, the interest of the consumer and the interest of your institutions are analogous.

Mr. KALLSTROM. Yes.

Chairman BACHUS. The National Retail Federation, Ms. Hanson, has also been very helpful in pointing out particularly some of the strengths of the uniform fair credit reporting system. I don't think there was a car dealer from my home State of Alabama who told me that he does business, about 20 percent of his business comes from the State of Florida, about 35 to 40 percent comes from the State of Georgia. The rest comes from the State of Alabama. He says even dealing with three sets of conflicting information could be a detriment in extending credit. So I think whether we are retailers or credit card companies or Ms. Duncan with the Consumers Union, I think we can certainly find some identity of interest because we are all looking for the same thing, and that is the extension of credit in a fast, expedient way.

It has been a great benefit if you look at low-and middle-income citizens, under FCRA there has been an explosion of available credit. At the same time, we ought to be able to find ways to protect those consumers in this process. So I think we all have an identity of interest there. We may have different opinions on how we get there.

At this time, I will yield back.

Mr. TIBERI. Thank you, Mr. Chairman.

We have a series of votes on the floor and the Chairman has asked me to recess the committee until 1:30 p.m. when we will return with the next panelist. Thank you.

[RECESS]

Mr. LATOURETTE. [Presiding.] The subcommittee will come back to order. We appreciate your patience during that series of votes,

and hopefully we will be able to complete this panel before more mischief like that is occasioned.

Ms. Duncan, I think we are with you, and thank you for being here. We look forward to your testimony.

STATEMENT OF JANELL MAYO DUNCAN, LEGISLATIVE AND REGULATORY COUNSEL, CONSUMERS UNION

Ms. DUNCAN. Thank you.

Good afternoon, Mr. Chairman and members of the subcommittee. Thank you for providing me with the opportunity to come before you today. I am Janell Mayo Duncan, Legislative and Regulatory Counsel for Consumers Union, publisher of Consumer Reports magazine. I am pleased to be able to share our views on the relationship between the FCRA and identity theft.

Consumers Union, an advocate for consumers, is the only consumer representative on this panel. We are a nonprofit organization, and as you will see from my comments today we would strongly disagree with Mr. Kallstrom's claim that he and MBNA are appropriate spokespersons for consumer interests.

In addition, the FCRA at its core is a consumer protection statute, and we are here and stand ready to join MBNA, MasterCard and the National Retail Federation in lending our perspective as the committee crafts legislation to address these problems, understand the impact on consumers, and to develop solutions to this crime.

This hearing is entitled Fighting Identity Theft, the Role of FCRA. We believe that the current operation of the FCRA, FCRA Federal preemptions, and ongoing industry practices are to a great extent responsible for the skyrocketing number of identity theft cases. Consumer Reports magazine looked at this problem in a 1997 article. At the time, the magazine described the crime of identity theft as one of the fastest growing in the nation.

The article chronicled stories of people victimized by the crime and in it we identified flaws in the system that we believed to be contributing to this problem, including lax identification standards, where credit is granted to a thief by creditors matching as few as two pieces of identification with information on the credit report of an unsuspecting individual; the granting of quick credit; the dissemination of convenience checks; instant credit and easy replacement of reportedly lost of stolen cards; inadequate fraud detection by credit reporting agencies or CRAs; credit grantors that ignored fraud warnings meant to serve as an obvious indication that an identity thief had been actively exploiting a consumer's credit file; and unfair correction processes where credit bureaus continue to update files with inaccurate information or information generated by the thief. Six years after our report, thieves have become more sophisticated and organized and the problems are more widespread. However, the basic elements placing consumers at risk have not changed and continue unabated. We believe that the solutions lie in requiring industry to better manage and safeguard information already at their disposal. In addition, the current preemption of State laws must be allowed to expire so that States can act quickly to address new and emerging identity theft crimes, be-

cause thus far States have been the most responsive and effective source of solutions to this growing problem.

Additionally, consumers must be empowered with more control over the dissemination of their personal information in order to prevent identity theft. Some of our specific recommendations are to allow consumers to obtain yearly and at no cost a copy of their credit report and credit score from the three major CRAs; prohibit CRAs from releasing consumer information unless they have made a careful matching of a minimum of four identifiers; require CRAs to notify consumers at their original address when an address change is made to their report; allow victims of identity theft to freeze their credit reports to prevent impostors from accessing any more credit in their names; penalize creditors that grant credit to a thief without following up on a fraud alert placed on a credit report; require CRAs to alert consumers free of charge when suspicious activity is observed on the report; increase penalties for furnishers that reinsert information in a consumer's credit file that already had been disputed by a consumer as inaccurate and had been previously removed; and give consumers control over the sharing of personal information among companies, including affiliates.

We urge this subcommittee to work to pass meaningful legislation that will address the elements of the FCRA and industry practices that help make the commission of these crimes possible. I have provided the subcommittee with additional recommendations in my written testimony. In our view, the improvements we suggest would go a long ways towards preventing this crime.

I thank the chairman and members of the subcommittee for this opportunity to testify and I look forward to answering any questions.

[The prepared statement of Janell Mayo Duncan can be found on page 109 in the appendix.]

Mr. LATOURETTE. I thank you very much for not only your testimony, but your ability to complete it before the red light went on. Thank you very much, Ms. Duncan.

Mr. Ansanelli, welcome and we look forward to hearing from you.

STATEMENT OF JOSEPH ANSANELLI, CEO, VONTU

Mr. ANSANELLI. Thank you and good afternoon.

My name is Joseph Ansanelli and I am the CEO and founder of Vontu. We provide information security software that helps guard against the loss of customer information. I am honored to provide testimony in fighting identity theft and the role of the Fair Credit Reporting Act. I commend the subcommittee for discussing this important issue.

My testimony draws from my experience in working with chief information security officers at some of the country's top financial services, insurance, media and retail companies. These security professionals are acutely aware of the challenges in adequately protecting consumer information.

To begin, we believe it is important to help a consumer quickly repair his or her credit when their identity has been stolen. However, this problem will continue to grow if we do not prevent the theft of consumer data in the first place. This means making sure

Social Security numbers, credit card numbers and other identifiers don't get out from those companies that have that information.

While there are many ways identity theft occurs, from a financial report taken from the trash, a credit card receipt in a restaurant, companies and government agencies are the ultimate sources for large electronic databases of consumer information. Without additional safeguards in place, millions of Americans may be victims of identity theft by the end of this decade.

Traditionally, organizations have focused on the hacker and preventing people from breaking into their customer data systems. Many organizations now realize that another significant threat exists. With the rapid adoption of the Internet and tools such as electronic mail, consumer information can be leaked in a moment's notice by insiders. No matter how secure an organization's systems are, many employees require access to sensitive customer data, yet it is much easier for insiders to accidentally leak or maliciously steal information than it is for a thief to break in from the outside.

As an example, in November of last year a customer service employee of Teledata Communications who had easy access to consumer credit reports, allegedly stole 30,000 customer records. That is the first step in the identity theft process. This theft cost millions of dollars in financial losses and demonstrates that even though any computer system can be hacked, it is much easier and in many cases far more damaging for information to be stolen from the inside. Last month, we conducted a survey with Harris Interactive of 500 employees and managers who had access to customer data that confirms this. Almost half of the respondents said it would be easy to take sensitive customer information from their employers's networks. Two-thirds believe that their coworkers pose the greatest risk to consumer data security, while only 10 percent said hackers were the biggest issue. In fighting identity theft, we suggest it is important to fix the problem and to look beyond external threats and recognize that insiders pose a fast-growing risk.

Based on our experiences, I recommend the subcommittee weigh the following when considering revisions to the Fair Credit Reporting Act. First, confusion is the enemy of consumer protection. A consistent and unified national approach to our credit system will benefit consumers the most. However well intentioned a system of 50 different laws might be, it would only create confusion and paralysis that would ultimately harm consumer protection. Therefore, we believe that the preemption provisions of the Fair Credit Reporting Act are critical and should extend to any additions to help protect identity theft.

Second, we urge the subcommittee to ensure that any modifications to the FCRA encourage companies to go above and beyond any stated requirements to protect customers' data. Most companies know it is in their self-interest to protect a customer's data. However, I have had companies question whether they should go beyond base Legislative and Regulatory requirements such as GLBA for fear in doing so could potentially reveal problems that trigger punitive actions. Future legislation should encourage and protect organizations that go above and beyond any base security requirements.

Third and most importantly, I suggest this committee develop a consumer data security standard as part of the FCRA. Ensuring a national unified and standard approach to protecting consumer information at its source will help to stop one of the main and growing sources of identity theft. Any such standard should include the following principles. First, corporate security policies should be mandated. A company security policy should be publicly available, regularly reviewed and updated, and audited and approved by its board of Directors. Second, employee education is critical. In the Harris survey I referenced earlier, almost one-third of workers and managers had not read or did not know if their company had a written customer data protection policy.

Third, data protection and control should require best practices. Physical and network protection should use best practices for all commercially reasonable solutions. And last, companies must enforce employee compliance. Organizations should have an obligation to regularly monitor and enforce employee compliance with government regulations and their own internal security policies for the use and distribution of sensitive consumer information.

I hope these comments will be helpful to the committee and I welcome the opportunity to answer any questions.

Thank you.

[The prepared statement of Joseph Ansanelli can be found on page 80 in the appendix.]

Mr. LATOURETTE. Thank you, Mr. Ansanelli.

Mr. Lundy, thank you for being here and we would like to hear from you.

STATEMENT OF LEE LUNDY, VICE PRESIDENT, CONSUMER SERVICES, EXPERIAN

Mr. LUNDY. Thank you, Mr. Chairman and committee members. Good afternoon.

My name is Lee Lundy. I am Vice President, Consumer Services, for Experian. I am responsible for managing Experian's National Consumer Assistance Center in Allen, Texas.

Of the total consumer reports that Experian issues each year, only about 1 percent results in a request by a consumer for disclosure. About half of that number results in an inquiry by a consumer relating to a dispute or a general question about a disclosure. Only a portion of this one-half of 1 percent results in an actual change to the consumer's file, which may be either a correction or an update. All of this takes place within an environment where the industry estimates that up to 30 percent of consumer contacts we receive are the result of credit-repairing inquiries where attempts are made to remove negative information, but it is accurate. These calls require investigative processes that impact our ability to address true consumer concerns. Today, I want to discuss the steps we are taking to provide the business community with ways to prevent ID theft, help consumers restore their reputation with victim assistance, and discuss solutions that will not work, specifically limiting information flows and providing free credit reports without condition.

What works? The most effective strategy is responsibly using the free flow of information. Experian and others are making large in-

vestments in developing effective fraud prevention and detection tools based on responsible information sharing. Our national fraud database is comprised of known and verified fraudulent activity provided by businesses from across many different industries. Our customers use this database to stop fraud before it happens.

Experian's Detect service takes fraud prevention to the next level by comparing an individual's application history for anomalies that may indicate fraud. Do they work? Just an example, one company using Experian's fraud tools experienced a 55 percent decrease in fraud losses and reduced the time it took to confirm fraud records by more than two-thirds. As you can see, fraud prevention is paramount. However, in the event that victim assistance is required, Experian has been working with our counterparts for several years to develop uniform and efficient processes. Recently, we announced a one-call fraud alert program. Today, consumers who believe they are victims of fraud need only contact one credit reporting agency to add fraud alerts and receive complimentary reports from all three of the agencies. Once the consumer receives the report, Experian's consumer assistance agents are trained to personally assist the consumer by explaining the information on the report and initiating an inquiry to the creditors to resolve any inaccuracies.

The question has been asked why it takes so long to resolve identity theft issues on a consumer's file. In some cases, the full extent of the crime may not be known for some time. Identity theft, unlike other crimes of theft, often occurs over a period of weeks or months. When a victim identifies fraudulent entries on a consumer report, we work promptly with the provider of the information to resolve the issue. So when you hear stories in the media that it took consumers months to unravel financial records affected by identity theft, it is often because elements of the crime do not fully appear until weeks or months after the criminal activity began.

What doesn't work? Restricting data access and providing free credit reports without condition. At face value, both seem to promise greater fraud protection. In reality, they do little to protect consumers and in fact may make the fraud problem worse. Access to and responsible use of information from a broad spectrum of sources is essential to our fight against fraud and identity theft. Effective solutions demand tools that utilize complete, accurate and current information from multiple sources in order to counter consistent variations of the crime. We know that more information, not less, will reduce fraud and ID theft. Eroding the ability of businesses to obtain, share and compare information will increase the risk of fraud and ID theft.

Free credit reports upon request have been touted as a solution to the fraud problem, but actually have little impact on fraud prevention and would impair our ability to control costs and meet mandated service levels. Current FCRA provisions already provide free reports for virtually all qualifying consumers. Costs such as postage, for the average report is approximately 13 pages long, and staff are often lost when factoring in the actual cost of a free report. Cases involving security breaches from systems outside of the credit allocation stream already result in large unpredictable numbers of free report requests. Such cases impose tremendous costs on credit reporting agencies. They also result in flooding our assist-

ance centers with calls that impact those consumers who have a more urgent service need.

Thank you for the opportunity to address the committee. I will be happy to answer any questions you may have. I have submitted a more detailed written statement for the record.

[The prepared statement of Lee Lundy can be found on page 134 in the appendix.]

Mr. LATOURETTE. I thank you, Mr. Lundy, very much. I think I will begin with you.

Obviously, as someone, and I think Mr. Sanders talked about legislation that he has drafted, and I know the legislation I have drafted with Mrs. Hooley has a provision that calls for one free credit report annually. So obviously it is disappointing to hear you opine that it actually would increase fraud activities. I think the only issue that I would take, well a couple of issues I will take with that statement.

One is that I don't think that it is being touted as the answer to identity theft. I think it is, to take another portion of your testimony, the more information the consumer has, I think, if it is a two-way street, if we are not only asking those who grant credit to be more vigilant, there is a concurrent responsibility on the individual, the consumer to pay attention, but they can't really pay attention if they don't know what is in their credit report. I think at least from my perspective, Mr. Sanders I know can speak for himself, but from my perspective that is the idea behind it.

So the question that I would have for you is, has the industry or has your organization calculated a cost and/or the ability to comply with such a provision should that be the ultimate enactment of the Congress?

Mr. LUNDY. Actually, I do not have those figures with me. We know that it is a tremendous impact only by what has happened in the recent past, as far as whenever we do have data stolen from within a business. We then get a very big impact as far as sending out free credit reports to consumers who really have not truly been impacted or affected by credit fraud, but only there is a fear that they may have been. It does create quite a bit of staffing issues because even with those additional calls coming in because of the literally hundreds of thousands of credit reports going out, we still are mandated to make sure that we handle all those calls within FCRA requirements.

Mr. LATOURETTE. Ms. Duncan, as I listened to your suggestions, I pulled some off the Web site relative to freezing credit reports and also it mentions increased participation by local police agencies in taking down reports. I think you mentioned three or four other things in your testimony today.

I am wondering if you have had a chance to review any of the legislation that has been introduced by any member of the Congress relative to fraud, and in particular I would think of Mr. Sanders's bill, I would think of Ms. Hooley's bill and any others, and whether your organization has formed an opinion as to whether they would work or are moving in the right direction, or we need to do more, or we are about there.

Ms. DUNCAN. We do agree that any additional information that can be given to consumers is a good idea, as consumers are being

asked to take control over their credit report and their financial well being. Yes, we have supported Mr. Sanders's legislation asking for a free credit report. We have been very active out in California supporting some of the laws that have come about out there. On the Federal level, we have supported other legislation that would require for the truncation of credit card numbers and quite a few others.

Mr. LATOURETTE. Okay. And I heard you take exception with Mr. Kallstrom's testimony, with Mr. Ansanelli sitting next to you. How do you feel about the preemption issue, the observation that having 50 different sets of credit regulations actually increases the opportunity for mischief? Has your organization taken a position on whether or not there should be Federal preemption in these areas?

Ms. DUNCAN. We have supported the expiration of the preemption provisions and we do believe that States have been very active in these areas. As you can see, there has been a lot of talk about the things that can be done, but as you know, the incidence of identity theft is skyrocketing, and the methods that criminals are using to perpetrate this crime are changing over time. So we think that States are probably the most appropriate body to act very quickly when these methods change.

Mr. LATOURETTE. Thank you.

Ms. Hanson, that brings me to your testimony and the question of preemption. As I understood you, you said that Federated has been pretty successful about getting to know your customer. One of the things I think you cited was you got to know your customer by information that had been shared by affiliates. If States come up with different rules and regulations to restrict sharing among affiliates, do you have an opinion as to whether or not that helps or hurts the problem we are discussing here today?

Ms. HANSON. I think it would make our job much more difficult as a retailer, to know our customer, if we have to wade through the morass of multiple States' different interpretation of laws. I think our job would become much more difficult in protecting our customers.

Mr. LATOURETTE. And Mr. Ansanelli, when a corporation decides to go above and beyond, or an organization decides to go above and beyond, were you talking about a benefit that basically would restrict them from liability should they, sort of protecting them from the lawyers?

Mr. ANSANELLI. Exactly. I don't like necessarily the phrase, but a safe harbor which is that they are actually going to try to find problems that they discover above and beyond what the regulation says. They should not then be held liable for finding out that they had a problem that they didn't have to actually go find to begin with.

Mr. LATOURETTE. That is an interesting idea. There is a company in my district that has nothing to do with what we are talking about, but a company in my district that disinfects things. When SARS was in the news, and it still continues to be in the news, they developed a program to disinfect the inside of airplanes. The airlines were reluctant to do it because by disinfecting the inside of the airline they might be assuming a responsibility that they don't currently have for passengers with SARS.

Thank you all very much.

Mr. Sanders?

Mr. SANDERS. Thank you, Mr. Chairman.

Before I get to identity theft, there is another issue that I would like to talk to MBNA about, and that is what some of us call the bait-and-switch process that many credit card companies are currently engaged in. Mr. Kallstrom, let me just read to you from an article that appeared in the New York Times, well, summarize an article that appeared in the New York Times on May 29.

The essence of the article was that it appears that all over this country companies, including your company, do a bait-and-switch. You send out solicitations to people asking them to accept your credit cards at certain interest rates, and then month after month these people pay the bill that they owe you. Let's say they have a 5 percent interest rate and they pay you every month the $200 that they owe you, whatever it is. Suddenly, lo and behold, 5 months later, after having paid on time every month what they owe you, the interest rates go sky high. And when they inquire as to why that is so, and many of them, of course, do not inquire. They don't notice what has been happening. They find out that somebody will tell them, well, yes, you paid us on time, but you borrowed additional money. We are sorry somebody in your house was sick and you needed additional money, and yes, you have always paid us on time, but nonetheless we are going to double or triple your interest rates.

Please explain to me why you think this is moral acceptable behavior when somebody month after month has paid you on time what they owe you? Why do you change the rules of the game and double or triple their interest rates?

Mr. KALLSTROM. I read that article in the New York Times also. For the record, I would say that we do not bait and switch. What we do is we assess risk and we give unsecured loans to people to better their life and to carry on or live in the world we live in today. I would not necessarily believe everything I read in the New York Times.

Mr. SANDERS. Well, let me ask you a question.

Mr. KALLSTROM. Let me finish my answer please. People's situations do change and we are assessing risk. There is a lot of oversight on us. There are a lot of good reasons, there are hundreds of reasons why we should assess risk.

Mr. SANDERS. Well, let me ask. I will give you your time. Sir, the problem here, as you know, is we are limited in time. I wish we had time.

Mr. KALLSTROM. Let me just finish the answer in 30 seconds.

Mr. SANDERS. Yes.

Mr. KALLSTROM. So from time to time, we do assess risk. We always pre-notify the customer as to the conditions that are going to change. We always give them the opportunity to just say no. We give them the opportunity to pay off that account at the existing rate and close their account, or keep the account open at the new rate that the risk has brought us to. That is good business practice, good ethical practice, and that is what we do.

Mr. SANDERS. What percentage of the people that you deal with who have your credit cards do you change interest rates on?

Mr. KALLSTROM. We are in a competitive market, sir, that changes all the time for competitive reasons.

Mr. SANDERS. I asked you a simple question.

Mr. KALLSTROM. I do not have an exact percentage.

Mr. SANDERS. And what percentage of the people do you think actually know? People get a lot of stuff. Among other things, they get 5 billion solicitations a year from credit card companies. What percentage of the people who you send out this information to do you think actually know?

Mr. KALLSTROM. I believe the vast majority on that point know because we highlight it. We set it off in sharp colors. But you are right about disclosures. People don't actually know what a lot of those things say, particularly the Gramm-Leach-Bliley ones because no one can understand what they say.

Mr. SANDERS. But I would suspect that many people who see their interest rates change, I want to get back. You say you are not into bait-and-switch, but what you are into is changing the interest rates on people even though they have paid you every single month. Now, if I do business with you and I pay my bill on time to you every month and I pay you what I owe you, why do you think you have the right to double my interest rate?

Mr. KALLSTROM. Because we must assess risk on the portfolio.

Mr. SANDERS. Even though I have paid you?

Mr. KALLSTROM. And you might have gone and borrowed $50,000 from somebody else and you are not paying it back. So in this day and age we live in, we have to look at the total.

Mr. SANDERS. In other words, what you are doing is punishing people who have paid their bills because you think they may not, even though they have always kept their word and their contract with you. I think that is wrong.

Mr. KALLSTROM. We are giving unsecured loans, sir, and we are giving them notice that if they do not want that additional rate; in every occasion, we are giving them notice.

Mr. SANDERS. Excuse me, excuse me, sir. You have not answered me in terms of how many people do not even know that their interest rates would change, and I suspect many do not.

Mr. KALLSTROM. I agree that the vast majority do know.

Mr. SANDERS. You are dealing with large numbers of people. Excuse me. Even if the vast majority is true, there will be many, many thousands of people who simply every month, who assume because they pay their bills on time, do not anticipate an increase in interest rate. I will bet you that there are thousands of people who are paying you far higher interest rates than they contemplated.

Mr. KALLSTROM. I don't know the percentage.

Mr. SANDERS. Thank you. I have limited time. I would love to discuss the issue. I really would, but we have a limited amount of time.

Mr. KALLSTROM. I would also.

Mr. SANDERS. Ms. Duncan, do you have thoughts on that practice?

Ms. DUNCAN. We agree with your concerns that there are consumers, and I read the article as well, out there who are, regardless of their payment history with the particular lender, are pos-

sibly seeing their rates skyrocket. Also, it is quite possible that that increase in rates, I mean, if you look at a consumer who has been responsible in the past, you could possibly assume that they would be responsible in the future. In making those rates go up like that, that could very well be the proverbial last straw that broke the camel's back.

Mr. SANDERS. Right. And there are instances, as I understand it, that that practice has driven people into bankruptcy. Thank you, Ms. Duncan.

Let me ask Mr. Lundy a question. When you discussed with the Chairman your opposition to providing consumers with free credit reports, you mentioned the cost. Obviously, there is a cost and we don't know what the cost will be. But how can you tell the consumers of this country that they are not entitled to free credit reports when just in 2002, MBNA just happened to have enough money in that year to pay their four top executives $308 million? Don't you think that maybe if they wanted to cover the cost of informing consumers all over this country what their credit reports were, maybe they could take a little bit of a cut in salary? Do you think that might be possible? Just a little bit. We don't want to put them on welfare, but $308 million for the top four execs, now, what can I say?

Mr. LUNDY. Sir, I can't discuss, of course, the salaries at MBNA. However, we are not opposed to free credit reports to consumers with conditions. We believe that all consumers knowing what is in their credit reports is very important. We do not believe that the price that we charge a consumer, which is $9 or less in some States, is prohibitive for consumers who have no conditions to actually get their credit file report.

Mr. SANDERS. I would certainly agree with you. It is not prohibitive. But there will be a heck of a lot of people who will not pay the $9 who, if they got it for free, might learn that they were a victim of identity fraud.

Let me get back to Mr. Kallstrom. Maybe you want to tell the people in terms of cost, what do you think about $308 million in 1 year for the top four executives?

Mr. KALLSTROM. Well, look, I don't know exactly what their compensation was.

Mr. SANDERS. I can give it to you.

Mr. KALLSTROM. I can tell you that is not salary.

Mr. SANDERS. That is total compensation.

Mr. KALLSTROM. Like Al Lerner who you talked about earlier, who is an American patriot, who served this country in Korea, who grew up in a back room and invested capital in a small company.

Mr. SANDERS. I am not making any disparaging remarks. Excuse me. We hear over and over again and we heard it from Mr. Lundy. I am not disparaging anybody or the patriotism of anybody. But there are a lot of Americans who are a little bit concerned, because they are going bankrupt in record numbers, about executive salaries.

Mr. KALLSTROM. Sir, with all due respect, those are not salaries.

Mr. SANDERS. Compensation packages is what I am talking about.

Mr. KALLSTROM. They are not salaries.

Mr. SANDERS. I said it five times, compensation packages.

Mr. KALLSTROM. They chose to sell some stock in the company that they built at the time, and you are taking a point in time and you are making a point.

Mr. SANDERS. That is right. I am making a point that in 2002, your top four executives made over $308 million.

Mr. KALLSTROM. It is not salaries.

Mr. SANDERS. Thank you.

Thank you, Mr. Chairman.

Mr. LATOURETTE. I thank the gentleman very much.

Mr. Toomey?

Mr. TOOMEY. Thank you, Mr. Chairman.

Mr. Kallstrom, just to follow up on this. I can't help but address this. I for one would be shocked and very concerned if you made credit decisions without taking into account the entirety of a person's credit portfolio. Just by way of clarification, with respect, for instance, to a corporate borrower, if you extend credit to a corporate borrower and that borrower were then to take on some massive new amount of debt after the fact, would the banking regulators be a bit concerned if that didn't cause you to reevaluate the loan that you had made, the terms of that loan?

Mr. KALLSTROM. Without question, the regulators would be extremely, well, they would find our practices outside the boundaries of their guidance clearly, in both of those instances. And that is why it is important to our economy that we do not have a lot of unsecured loans out there at high risk. There is a reason why this happens. There is a good sensible reason why it happens.

Mr. TOOMEY. Right. What I would like to focus on, I just wanted to establish that point, but I did want to focus back on the issue at hand of identity theft. Can you tell us, for your institution, and if this is in your testimony, I apologize, I did not see it though, has the cost to your bank been rising or falling with regard to incidents of identity theft and the fraud related thereto?

Mr. KALLSTROM. I think generally they have been rising. Even though we still have some of the lowest rates in the industry, they are still rising.

Mr. TOOMEY. Do you see that as just a cost of doing business, or are you, in the face of this rising cost, and that was the way I thought you would respond, are you developing new procedures and systems for more aggressive prevention?

Mr. KALLSTROM. We are, but as we talked about earlier, this whole thing is geometric. It involves law enforcement. It involves the credit bureaus. It involves retailers. It involves the credit industry. It involves consumers. It involves the fact that we have an epidemic of false identification in the world and in the United States, where 8-year-old kids can make driver's licenses on a laptop computer. So it involves a lot of different things.

Mr. TOOMEY. I understand that and I acknowledge that, but it seems to me that ultimately a lot of the problem arises from financial institutions that extend credit to people who are pretending to be someone that they are not.

Mr. KALLSTROM. Without question, that is correct.

Mr. TOOMEY. So it seems to me that the point at which we are most likely to be successful in preventing this would be systems

that defeat that attempt. Since the incidence of this fraud is rising so much, my question is what new things are you folks working on, is the industry working on that will cause that graph to turn around and have the same precipitous decline that we need to have?

Mr. KALLSTROM. I think clearly the more information we have, the fact that we have affiliates and affiliates were created for good reason, and we can have more points of information. Our neuro-network can be a lot more effective and we can stop identity theft to a much larger degree. But there are forces outside our control that must simultaneously improve.

Mr. TOOMEY. I am not suggesting that this is all your responsibility to solve this. I am acknowledging that there are other aspects of this problem. But for instance, does it make sense for financial institutions such as yours to have considerably more aggressive identification verification procedures when new accounts are established, or some substantive change is made in an account?

Mr. KALLSTROM. Yes, it does, sir. And we invest a lot of technology in that area. We invest a lot of human resources in that area. I would just make a point, at the point of sale, if someone comes in an presents baseline documents that are recognized in the United States as being prima facie evidence of identity, birth certificates, Social Security cards et cetera, in true name and in true address, it is very difficult to weed those types of events out. There is technology available today to stop that practice. I would encourage the Federal government to deal with that issue.

Mr. TOOMEY. If we could just follow up on that. When people provide that, obviously it is happening that people are providing that information and it is all information about someone else.

Mr. KALLSTROM. Right.

Mr. TOOMEY. And then some portion of it is usually inaccurate, like an address, perhaps. What about using much more aggressive techniques to verify these things, some kind of biometric signature or some kind of verification when this person's name comes up?

Mr. KALLSTROM. I agree, and I think our processes, our expert systems, our neuro-network, our human beings, our fraud experts, the way those situations get routed, we stop the vast majority of them. Our identity theft percentage is extremely low. But yes, we need to have biometrics. We need to have anti-counterfeiting technology put into our baseline identification documents. So I am agreeing with what you just said.

Mr. TOOMEY. Do you have any specific biometric techniques that you think are likely to be implemented soon?

Mr. KALLSTROM. Today in driver's licenses in the United States, there are about 20 different biometric algorithms in the licenses. There is technology available today in one black box that can identify all of those. So we could have at a point of sale a black box that could say green light-red light as to whether that identification is counterfeit. I think the other thing that helps us immensely is having many data points to check, so that someone showing up with your driver's license and your address with their picture on it, we are going to know that they are phony because we are going to check other points of reference that you cannot answer those questions.

Mr. TOOMEY. If the Chair would just allow for a wrap-up comment, I thank you for that. It just strikes me that when we hear the kind of horror stories that we are hearing and we know that the frequency of these incidents is increasing, my concern is that if the industry does not take very aggressive measures to successfully change the trend, there will be legislation which might become very onerous at some point, that may have unintended consequences. I am just strongly encouraging you.

Mr. KALLSTROM. I agree with that. I would just simply say the industry is spending millions of dollars in this area, hundreds of millions of dollars in this area.

Mr. TOOMEY. Okay. Thank you, Mr. Chairman.

Mr. LATOURETTE. I thank the gentleman.

Mr. Moore?

Mr. MOORE. Thank you, Mr. Chairman.

Mr. Kallstrom, in your written testimony you said, and I believe you testified this, everyone agrees it would be of enormous benefit to provide consumers with easily digestible privacy notices that include easy opt-out procedures. Is that correct, sir?

Mr. KALLSTROM. Yes, sir.

Mr. MOORE. Why then are the notices that we receive, every person in this country receives, from a credit card company so hard to read and so, I am a lawyer; I practiced law for 28 year and I do not read those. Why are they so complicated?

Mr. KALLSTROM. In the 1999 Gramm-Leach-Bliley Act, the regulators did not create a model notice for the safe harbor. So all the lawyers from all the regulators, I mean good people get in a room and came up with these notices that basically talk about technical compliance, but I think they have largely left the consumers bewildered as to what they mean. They are four or five pages long. The type, you know, you get my age, it is very difficult to read. They are in legalese that virtually nobody, in my view, understands.

I think a much better solution would be to, and I would think my friend from Vermont would agree, tell consumers what their rights are in plain English on a short notice, and then give them a very simple way of opting out if they do not want to share information. That is what consumers want.

Mr. MOORE. And you don't have a problem with opting out if they make that choice, the consumers?

Mr. KALLSTROM. No. I think consumers should be given their choices in plain English and they should be allowed a simple methodology to opt out. We would hope that the majority would not opt out because we think some of the offers would be compelling. If you have business with us and you manage your business very well, your unsecured loan, and we have another product that we are going to price you at very competitively, we would think you would want to know that. But there will be some people that clearly will opt out and that is fine.

Mr. MOORE. And they have that right if they choose, correct?

Mr. KALLSTROM. Absolutely.

Mr. MOORE. All right. Do you have any kind of form, simplified notice?

Mr. KALLSTROM. Actually, we had a working group of people in the industry and we have come up with some examples of what

these forms would look like. They have gotten wide distribution. I would be happy to attach them to my statement and leave them here for the committee. But one form is sort of modeled after a food can nutrition label.

Mr. MOORE. Is this such a form?

Mr. KALLSTROM. Yes.

Mr. MOORE. Can you see it? It says "version K." Would that be it?

Mr. KALLSTROM. Yes, sir.

Mr. MOORE. Mr. Chairman, I would ask that a copy of this be received in the record.

Mr. LATOURETTE. Without objection.

[The following information can be found on page 210 in the appendix.]

Mr. MOORE. Thank you.

Are you aware of any efforts by individual State legislatures to change notice requirements? What is your opinion about that? Of what consequence is that?

Mr. KALLSTROM. As we sit here today, sir, there 39 States considering 154 Gramm-Leach-Bliley-type related bills today. There are 46 States considering 234 FCRA-type bills today.

Mr. MOORE. What would be the consequence as far as you are concerned for providing credit at a fair price to consumers if that were the case?

Mr. KALLSTROM. I think clearly the balkanization of our system would have higher prices, higher interest rates. My friend from Vermont would be more exercised than he is today because things would be much higher. The European Community is trying to mimic our system over there, and we are talking about balkanizing our system. It would have dramatic negative impacts on our economy. I think it would have the most debilitating impacts on the lower rung of our economic population, who are finding their way into credit, who are getting the credit card, opening a small business with a credit card, building a credit file. Those segments of zip codes in different areas that in prior times were not issued good credit or good offers or preapproved offers, where they could pick from one or two different offers, they would be the most harmed, without question. There are economic studies that clearly point that out.

Mr. MOORE. Would it be correct, Mr. Kallstrom, that a populated State like California or New York or some other State with a large population, by enactment of some of these provisions might in effect control what happens in a lot of other States?

Mr. KALLSTROM. I think there will be standards, congressman, in these areas. The question is, will they be standards set here in Washington that benefit the entire country, or will they be California standards that become the de facto national standard. I think that would be a sad day for business and for our economy, and would not help our country, would not help the lower quadrant of the FICO-scored people that are clawing their way up into the middle class. It would have a negative impact on small business and it is not the right thing to do for the good of this country.

Mr. MOORE. You say it would hurt the economy. How so?

Mr. KALLSTROM. I think it would have a dramatic impact on credit. It would close out that community I talked about. It would have an impact on our GNP. It would have an impact on consumer spending. Rates would be higher. Clearly, rates would be higher and there would be less credit available.

Mr. MOORE. I am concerned about opening up GLB and the problems that could present from the standpoint of building bipartisan support for FCRA. I am also concerned that my constituents could get something far worse if GLB is opened up again and something happens there. Do you have any of these concerns?

Mr. KALLSTROM. We certainly have concerns. We think, though, that when you talk about the whole issue of privacy, the majority of people in focus groups talk about identity theft. They talk about issues of simplicity of notice. We think the way to go here is to give people plain English notice and to give them an easy methodology to opt out. If they want to restrict the information at businesses, that is what they should do. I think by the government doing nothing in that area and allowing the States to muck around and balkanize this whole area, we are going to end up with national standards, but they are not going to be Federal standards. And States are not going to spend the money to cookie-cutter a little different version of a standard in 50 different States. They are going to go with probably the California standard, the most restrictive, and we are going to let Sacramento decide what the Federal policy is going to be, as opposed to the Federal government.

Mr. MOORE. Thank you, sir.

Ms. DUNCAN. I would like to respond.

Mr. MOORE. I would like to hear your response. Mr. Chairman, is that okay?

Mr. LATOURETTE. Sure.

Ms. DUNCAN. From the perspective of opting out, the Gramm-Leach-Bliley notices only informs people of their rights, but for the most part consumers are only allowed to opt out of third party sharing. I would be very surprised if what Mr. Kallstrom is referring to in being in favor of allowing consumers to opt out would be extended to letting them opt out of the sharing of their information between affiliates. That is something that I think consumers should have more power over, the sharing of their personal information. If they share it with an entity for one purpose, it should not be able to be used unauthorized for other purposes.

Mr. MOORE. Okay. Would you agree, though, with the general statement that any solution should help consumers make more informed decisions about information sharing and that everyone agrees it would be of enormous benefit to provide consumer easily digestible privacy notices that include easy opt-out procedures. Would you agree with that generally?

Ms. DUNCAN. More comprehensible is always better. Easier is always better. Meaningful is more important. What I am trying to convey is that these notices, the rights are not meaningful so the notices are not meaningful because it is not giving consumers the ability to opt out of sharing between joint marketing partners and affiliates.

Mr. KALLSTROM. They are not meaningful because they are not understood.

Ms. DUNCAN. And they are not meaningful in that what is being conveyed are not true rights, but just a notice of how we are going to use your information regardless of whether you like it or not.

Mr. MOORE. Have you seen the proposed sample simple notice?

Ms. DUNCAN. I have heard about it. I have not seen it yet. My concern also is that regardless of simplicity, which is important, what is more important is to have the rights be meaningful.

Mr. MOORE. If they are following the law, is that sufficient? My question is, if they are following the law, is that a good thing? And if it is understandable to the consumer?

Ms. DUNCAN. The consumers in California have been polled and show that they do not believe they are being given enough rights under the current law.

Mr. MOORE. That is not the question. The question is, if whoever the provider of credit is tells them what the law is and tells them what their rights are in an understandable fashion, is that something that is good?

Ms. DUNCAN. To follow the law is good, yes.

Mr. MOORE. And advise them in simple language what the law is and what their rights are, is that good as well?

Ms. DUNCAN. Or course. That is certainly always a positive thing.

Mr. MOORE. Thank you.

Mr. LATOURETTE. I thank the gentleman.

Mr. Tiberi?

Mr. TIBERI. Thank you, Mr. Chairman.

I would like to submit for the record an editorial that was in The Hill publication today.

Mr. LATOURETTE. Without objection.

[The following information can be found on page 212 in the appendix.]

Mr. TIBERI. Thank you, Mr. Chairman.

Mr. Kallstrom, I am going to continue along the lines of questioning that Mr. Sanders started and Mr. Moore continued. Are you familiar with the legislation that was introduced by myself and Mr. Lucas dealing with national uniform privacy standards?

Mr. KALLSTROM. I am, sir.

Mr. TIBERI. Good. You had in answering a question that Mr. Sanders had asked you, you started down the road of explaining how privacy notices were complicated and confusing to consumers under Gramm-Leach-Bliley. You did not finish. Can you expand on that?

Mr. KALLSTROM. Yes, I think the Gramm-Leach-Bliley notices, because there was not a simple model notice created, the lawyers, which they should do to protect everybody, created this monster of a notice that virtually nobody can understand. Even some lawyers can't understand it. So it is no question that there is a lot of consternation. There are a lot of people that think these things are created by the companies and on purpose so people cannot understand their rights. Nothing could be further from the truth. Those notices are created by Gramm-Leach-Bliley and the regulators getting together and creating this five-page notice that is written in type that you can barely read.

So it does not surprise us that people have all this consternation about what their rights are. We think one solution, a simple solution is to give them a plain English version. Not a version, we would always make available the long notice so they could if they wanted to get a master's degree in law, they could figure out what it means.

Mr. TIBERI. You mentioned 30 States have legislation introduced that deal with this issue.

Mr. KALLSTROM. Thirty-nine States.

Mr. TIBERI. Thirty-nine States. What happens on this particular issue if States begin passing their legislation?

Mr. KALLSTROM. What you end up getting is you get different versions of the same thing, with separate notices that say basically the same thing, but they are different. We have a bill in California now, SB-1, that has a separate notice that probably ends up saying virtually the same thing, but it says it in California language. The cost of sending out multiple notices would be more confusing, not less confusing. So we think the solution is to settle on some plain simple language on a simple meaningful way of opting out very easy. You call an 800 number. You fill out this thing, just like changing your address, and you opt out. And to her point, we give them real choices of what the law is to opt out of. We think that is the solution.

At the same time, make some fixes for identity theft, which we talked about for hours all the different things that can be done to make that more effective. I think that is what is on the minds of consumers.

Mr. TIBERI. I want to get to identity theft, but before we go there expand upon your comments with respect to the current relationship between Gramm-Leach-Bliley and FCRA as it applies to State laws on affiliate sharing.

Mr. KALLSTROM. Yes, we think that FCRA is the rule on affiliate sharing and governs affiliate sharing. Let's remember, we created affiliates and we let companies have affiliates for a couple of reasons. First reason probably, to better manage risk; to get parts of the company, and in our company we have five affiliates. One of them is a technology or data processing company. We have to share information with them or else they could not process the information. So we can look at these things and put all those entities that we really deal with risk in one place.

Of course, we created these affiliates so that people with good credit, even people with marginal credit, could get better offers for other products. That was the whole idea, the idea of a rising tide raising all ships in the harbor; that if you did business with company X in one particular line, now you needed a home equity loan or you needed some other product, they had the benefit of having advantages of your ability to manage debt and they could take that good record that hopefully you had and they could apply it to good costing, good interest rates over here so that people could emerge and have success in the American dream. It was done for those reasons. It was not done for any dastardly reason that people would paint it as today.

Mr. TIBERI. Final question, each State has a different criminal background check system. How, in your mind, does the reporting

of that information, without a national uniform standard, impact your customers and your employees?

Mr. KALLSTROM. Well, it is complicating. I don't mean to get involved in 9-11, my other job I have, but this business of connecting the dots is always universally more difficult when you have stovepipe information, when you have information that is not easily accessible or quickly accessible. So for the reasons that we can have a good credit system that is national, we can therefore have the benefit of it. People have got to remember, it was not that long ago you waited five weeks to get a mortgage. It wasn't that long ago that if you wanted cash, you had to go to your bank and write a check. You didn't go to an ATM. There was no such thing. And if you drove from Vermont to Florida, that credit didn't necessarily follow you. You had to start all over again. So the American public, with all the problems we have here, and identity theft is a huge problem, but we think it is fixable. With all the problems we have, we have the best system in the world.

Mr. TIBERI. Thank you.

Ms. HANSON. Could I add a comment on the subject of GLB and Mr. Kallstrom's testimony on that?

Mr. LATOURETTE. Sure.

Ms. HANSON. Just generally speaking, all good discussion, good ideas. I think everybody is generally in agreement that it is a complicated notice, hard to understand for our customers, but the FCRA and the issue that is at hand is of such high priority to us. I share your concern that introducing another subject at this point will just complicate an already complicated subject. We are very concerned about that.

Mr. LATOURETTE. I thank you.

Mr. KALLSTROM. Let me add, extending FCRA is our number one priority, clearly, too, but we would be less than honest if we did not talk about a companion issue that is interwoven with FCRA. The devil is going to pay its due here in the future if we balkanize the other half of the system.

Mr. LATOURETTE. Okay. I thank you, Mr. Tiberi, and the six of you. I thank you very much.

Mr. SANDERS. Are we letting them off so easily?

Mr. LATOURETTE. Well, we have been here a long time, Mr. Sanders.

Mr. SANDERS. I know that Mr. Kallstrom wants more questions.

[LAUGHTER]

Mr. LATOURETTE. Maybe you and Mr. Kallstrom can talk in the hallway a little bit.

Mr. SANDERS. Do you have a few more minutes or do you want to close it?

Mr. LATOURETTE. I really was going to close it up. If you have a couple of questions you want to ask, I am happy to yield.

Mr. SANDERS. If you would.

Mr. LATOURETTE. Sure.

Mr. SANDERS. Okay.

Just a few points for the record, picking up on Mr. Moore's question, the first point that we have to deal with when we talk about preemption and States's rights, we live in a Federalist society. We have local government, State government and Federal government.

In fact, if we really want a very simple effective system, we could have a dictator sitting a few blocks away from here, wipe out State government, everything would be nice and simple. Very few of us want to live in that society.

We live in a society where different States have different regulations for how fast you can drive your car and a dozen other things. We call that American democracy. That is what we call it. Does it cause problems sometimes? Yes, it does. But the other side of that is that sometimes somewhere in California or in Vermont or in New Hampshire, some attorney general or some member of the legislature or some governor comes up with a great idea and it works in that State, and other States steal that idea and eventually it filters here to Washington, D.C. and it becomes the law of the land. Many of my conservative friends say that all the time. They say States are the laboratories of democracy. My friend is nodding his head in agreement.

So some of us get a little bit confused when our conservative friends on Tuesdays or Wednesdays tell us they want the big bad Federal government, which they knock on Mondays and Fridays as terrible, to limit the ability of States to protect consumers. That is one point.

Second point, just for the record, I think Mr. Kallstrom if my memory is correct you indicated that if we have States moving in different directions, their interest rates might be higher. Did you say that? I think you said that.

Mr. KALLSTROM. I think the impact would be that there would be more costs in the system. Clearly, that is the case.

Mr. SANDERS. Well, let me tell you what the case is. As a result of the 1996 Fair Credit Reporting Act amendments, they exempted stronger consumer protection statutes in California, Massachusetts and Vermont from preemption. So we still have those laws. What we have seen in those three States is very low bankruptcy rates. In fact, Vermont now has the lowest rate of consumer bankruptcies in the country. And also in terms of mortgage rates, the most recent data indicates that the State of California has the lowest effective rate of a conventional mortgage in the nation, and Vermont and Massachusetts are well below the median. Those are States that have the rights, and you were suggesting this would be a terrible thing, but those States have done okay.

The last question that I would ask is you suggested, Mr. Kallstrom, that that legalese, and I certainly agree with you that you have very complicated language that was developed by lawyers, but those were developed by your lawyers, the industry's lawyers.

Mr. KALLSTROM. The regulators, sir.

Mr. SANDERS. Well, then you will have to tell me why it is that credit unions operating under the same law have much simpler language.

Mr. KALLSTROM. I can't answer that question. I don't know the answer to that. Logically, I am told, and I stand to be corrected, that the bulk of the work was done by lawyers representing the seven different regulators. I am sure there was input from the industry. Clearly, I am sure there was. The bottom line is they are not understandable.

Mr. SANDERS. Right. We certainly agree on that, and to the best of my knowledge credit unions operating under the same law and the same regulations have easily understood language. You might want to look into that, sir.

Mr. KALLSTROM. I will look that up.

Mr. SANDERS. Okay. Thank you.

Thank you, Mr. Chairman.

Mr. LATOURETTE. I thank the gentleman very much. I would just editorially comment that some of us on our side sometimes wonder why members of your party are champions for the Federal government on Monday, Wednesday and Friday and champions for States's rights on Tuesday and Thursday.

[LAUGHTER]

Mr. SANDERS. I am an Independent, so my party is always consistent. They always do what I say.

[LAUGHTER]

Mr. LATOURETTE. I thank the gentleman very much.

The chair would note that some members, like Mr. Sanders or others, may have additional questions for the panel which they would like to submit in writing. Without objection, the hearing record will remain open for 30 days for members to submit written questions to these witnesses and to place their responses in the record. Again, it has been a lengthy hearing. We thank you for your patience and we thank you for your participation.

The hearing is adjourned.

[Whereupon, at 2:38 p.m., the subcommittee was adjourned.]

A P P E N D I X

June 24, 2003

STATEMENT OF CHAIRMAN SPENCER BACHUS
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT
"FIGHTING IDENTITY THEFT – THE ROLE OF FCRA"

Good morning. The Subcommittee will come to order. Our hearing today about the role of the Fair Credit Reporting Act, or FCRA, in fighting identity theft is the sixth in the series of hearings this Subcommittee is holding on FCRA. The provisions in the FCRA that guarantee a single national standard are set to expire on January 1, 2004. We have previously held hearings covering the importance of a national uniform credit reporting system to consumers and the economy and more specifically on how FCRA helps consumers obtain more affordable mortgages and credit in a timely and efficient manner. At our last hearing, we discussed the role of the FCRA in employee background checks and the collection of medical information. Today we will focus on the important issue of identity theft.

This hearing consists of three panels. Our first panel is made up of federal and state law enforcement officials who will inform us about ongoing efforts to apprehend and prosecute identity thieves. Our second panel includes two victims of identity theft who will share their personal experiences with this crime. I appreciate their courage and willingness to appear before us today. Our final panel includes several representatives from the financial services industry who will share their perspectives on the FCRA and identity theft.

Identity theft is a crime committed by individuals or organizations seeking to capitalize on the good name of an innocent and unknowing consumer. It is a particularly heinous crime that harms consumers and financial institutions alike. A typical instance of identity theft involves a criminal using the personal data of another individual to assume that individual's

identity. Using the false identity, the criminal will obtain goods or services charged against the victim's credit. The identity thief may also commit additional crimes using the victim's name, creating an arrest record for the victim. These activities obviously tarnish the victim's reputation, credit history, and sense of security. The victim of identity theft must then make a great effort to get his or her credit report and personal history back in good shape. Because the financial losses associated with identity theft are generally the burden of financial institutions and other businesses, not the consumer, financial institutions are also victims of identity theft.

Although statistics on identity theft are not widely available, the problem appears to be growing. In March 2002, GAO noted that there is "[n]o single hotline or database [that] captures the universe of identity theft victims. Some individuals do not even know that they have been victimized until months after the fact, and some known victims may choose not to report to police, credit bureaus, or established hotlines. Thus, it is difficult to fully or accurately quantify the prevalence of identity theft." Nonetheless, the GAO noted that "the prevalence and cost of identity theft seem to be increasing, according to the available data that we reviewed and many officials of the public and private sector entities we contacted." Moreover, according to the Federal Trade Commission, identity theft is the most common complaint from consumers in all fifty states, and complaints regarding identity theft have grown over the last three years.

Existing federal law does address the issue of identity theft. For example, the Identity Theft and Assumption Deterrence Act prohibits the transferring or using another person's identity for fraudulent or other illegal activities. Federal law also makes it illegal to use or traffic in counterfeit credit cards and debit cards and prohibits criminals from attempting to obtain customer identification and other consumer information from financial institutions under false pretenses.

The FCRA also is an important tool in addressing identity theft issues. Financial institutions frequently find that the consumer reports they are able to obtain from credit bureaus under the FCRA provide the most useful information in attempting to distinguish an identity thief from a legitimate consumer. For example, discrepancies between an address or social security number contained in a consumer report and the information contained on an application can be used to identify and prevent an identity theft before it occurs. In addition, an identity thief who knowingly and willfully obtains a consumer report from a consumer reporting agency under false pretenses is subject to criminal penalties under the FCRA.

The FCRA also plays a central role in mitigating the consumer harms associated with identity theft. Under the FCRA, each consumer has the right to review the contents of his or her credit report at no cost and determine whether any fraudulent activity has been attributed to the consumer's credit file. If a consumer has been a victim of identity theft which results in misinformation appearing on the consumer's credit report, the FCRA establishes the mechanism whereby the consumer can notify the credit bureau of the fraudulent information and have that information deleted.

I believe today's hearing will be especially useful with respect to the Subcommittee's legislative agenda. It is my firm intent that we address the issue of identity theft and assist consumers in feeling more secure about the use of their personal information. Although today we will hear about the role of the FCRA in fighting identity theft, I am particularly interested in how the national standards established by certain provisions of the FCRA relate to fighting identity theft. For example, would credit bureaus have an easier time resolving alleged cases of identity theft under a single standard or under 50 different standards? Would identity theft increase if credit or insurance could not be offered through prescreening on a nationwide basis?

Could financial institutions rely on credit reports as a fraud prevention tool if the contents of each credit report varied by state, or if furnishers ceased to provide quality information to credit bureaus? Would restrictions on affiliate sharing result in increased identity theft? These are all important questions directly related to the national standards established by the FCRA.

I want to thank Chairman Oxley, Ranking Member Frank, and Mr. Sanders for working with me on FCRA reauthorization. The Chairman has announced that it is the Committee's goal to introduce and markup FCRA legislation over the next few weeks. I look forward to working with him, the Ranking Member and members of this subcommittee on this important piece of legislation.

The chair now recognizes the Ranking Member of the Subcommittee, Mr. Sanders, for any opening statement he would like to make.

June 24, 2003

Opening Statement by Congressman Paul E. Gillmor
House Financial Services Committee
Subcommittee on Financial Institutions and Consumer Credit Hearing entitled, "Fighting Identity Theft – The Role of FCRA"

Thank you, Mr. Chairman, for holding this important hearing. I appreciate this subcommittee's thorough examination of all the issues surrounding the Fair Credit Reporting Act (FCRA). I continue to believe that ensuring a uniform national standard for consumer protections governing credit transactions is one of the most important tasks this committee will face in the 108th Congress.

As we are all now aware, on January 1, 2004 these standards as established in the FCRA will expire and states will again have the ability to enact differing regulations. Congress enacted the FCRA in 1970, to bring the consumer credit reporting industry under Federal regulation and to create a uniform system of rights governing credit reporting transaction. This mandate has been incredibly successful and allowed for the creation of the sophisticated system we have today. It has greatly expanded consumer access to credit and allowing individual states to enact their own standards would undoubtedly risk its collapse.

The risk of identity theft is of great concern to me. Throughout my years in Congress, I have been a strong supporter of personal privacy especially regarding financial information. Victims of identity theft may not even know they have been targeted until significant, possibly irreparable, damage has been done to their financial profile.

I am happy to be an original cosponsor of the Identity Theft and Financial Privacy Protection Act (HR2035) to combat this increasing problem. This legislation would impose requirements on credit card issuers to help protect against fraudulent change of address notices, codify the use of fraud alerts in credit reports, require the truncation of credit and debit card numbers for many record keeping purposes, and allow consumers to obtain one free credit report from each consumer reporting agency per year.

Thank you again, Mr. Chairman, for allowing us to debate this important issue. I look forward to an informative session.

OPENING REMARKS FOR THE HONORABLE RUBEN HINOJOSA
HOUSE FINANCIAL SERVICES COMMITTEE
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT
"FIGHTING IDENTITY THEFT -- THE ROLE OF FCRA"
JUNE 24, 2003

Chairman Bachus and Ranking Member Sanders,

I want to thank you for holding this final non-legislative hearing today to investigate the role of the Fair Credit Reporting Act in fighting Identity Theft. It is necessary that we continue to assess the importance of the national credit reporting system. I look forward to this hearing and the series of hearings this Subcommittee will hold to further clarify the issue.

As I noted at the first hearing, my office was contacted frequently by numerous individuals and groups about the Fair Credit Reporting Act in the first half of this year. I personally heard from industry, consumer groups and several regulators on this issue. Lately, I have not been contacted by industry groups or consumer groups on what they would like included in legislation that likely will be crafted and introduced in the near future. It is my hope that Treasury and the Administration will publish its long-awaited proposals on Identity Theft and the FCRA, perhaps as soon as this week. Most of us realize that language has been available at the Treasury Department, but the White House has been taking its time deciding what position to take on Treasury's proposal while also watching closely the developments in the House and the hearings in the Senate.

In 2001, more than 117,000 complaints from identity theft victims were added to the FTC's database, the Identity Theft Data Clearinghouse. In 2002, those complaints increased by almost 162,000. According to FTC Chairman Beales, the dramatic increase may reflect a growing awareness of consumers about identity theft. Consumers who call the FTC hotline receive telephone counseling from specially trained personnel who provide general information about identity theft and help guide victims through the steps needed to resolve the problems resulting from the misuse of their identities. Consumer are advised to contact the three national consumer reporting agencies and have a fraud alert placed in their file; close accounts identity thieves have accessed and dispute unauthorized charges; and report the theft to the police and get a police report.

Identity theft occurs when a consumer's social security number, credit card number, or name is used without his or her knowledge to open fraudulent credit, telecommunications, or utility accounts-or to use already existing accounts. It can also occur when an individual's name is used unknowingly to pass bad checks, or to get loans, jobs, or obtain housing.

This crime potentially affects every consumer and all sectors of the financial services industry including financial institutions, credit card companies, insurance companies, mortgage companies and hospitals. The theft can be carried out over the telephone, by computer hacking into an individual's confidential files, or by stealing hard copies of a company's billing information. The victim of the theft usually doesn't realize the information has been stolen until some time later. As a result these crimes could be used to support terrorism, among other criminal activities.

Today, I cosponsored H.R. 2035, the `Identity Theft and Financial Privacy Protection Act of 2003,' introduced by Congresswoman Hooley, the Chair of the Democratic Task Force on Identity Theft on which I serve. The Task Force investigated the exploding problem of identity theft, the fastest-growing white-collar crime in America, and other financial crimes. I decided to cosponsor Congresswoman Hooley's legislation because it contains strong provisions that will help fight identity theft. Those provisions include:

- amending the Truth in Lending Act to require credit card companies that receive a request for a new card less than 30 days after they have received a notification of a change of address for the same account to notify the cardholder at both the new and old address using rules prescribed by the Fed, thus allowing issuers to adapt to changing technologies;

-codifying the voluntary practice of credit reporting agencies to include a "fraud alert" in the file of a consumer at the consumers request;

-requiring credit reporting agencies to investigate discrepancies between creditor information and credit bureau information;

-requiring that by January 2006 all electronically printed credit card receipts are truncated so that only the last five digits of the card number are printed; and,

-requiring credit reporting agencies to distribute one free credit report annually to each American consumer at their request.

These provisions and this bill are extremely important to Texas, which ranks third in the number of Identity Theft complaints reported to the FTC.

I have said in the past that one of the main decisions we, as a Committee, needed to make is whether to extend all seven exceptions to the Fair Credit Reporting Act that preempt state law, just some of the exceptions, or none of them. They all expire January 1, 2004.

On June 11, 2003, I and several New Democrats cosigned a letter to Chairman Oxley and Ranking Member Frank looking towards their leadership to ensure that legislation extending the seven expiring provisions of the Fair Credit Reporting Act (FCRA) is passed by the House and Senate before their termination on January 1st of next year. I believe that these seven provisions enhance the efficiency of the nation's credit system, promote access to the financial industry, protect American consumers, and I am firmly committed to extending them.

In turn, we sent a letter to Treasury Secretary Snow and to the White House asking them to finally propose their FCRA and Identity Theft legislation. To date, we have yet to receive a response.

As our letter to Chairman Oxley and to Ranking Member Frank states, it is imperative that any legislation that the Majority introduces or the Administration produces address the following issues:

- Identity theft prevention and mitigation;
- The expeditious handling of consumer complaints and disputes;
- Greater accuracy in credit reports; and,
- Consumers' access to their credit information.

As I have stated before, I will continue to work with all interested parties to ensure that the final legislation is balanced and fair. I look forward to today's testimony and to the legislative hearings to follow in July.

Statement Congresswoman Sue Kelly
Subcommittee on Financial Institutions and Consumer Credit
Hearing: "Fighting Identity Theft – The Role of FCRA"
June 24, 2003

Thank you, Chairman Bachus, for holding this important hearing on the role of the Fair Credit Reporting Act (FCRA) in preventing identity theft.

Earlier this year, I chaired a joint hearing with Chairman Bachus on fighting identity fraud and improving information security. In that hearing, we learned that identity theft is among the fastest growing crimes in America, and it is top consumer complaint according to the Federal Trade Commission. Most importantly, we discovered that combating identity theft requires the collaborative effort of law enforcement and regulatory agencies, consumers and financial institutions – all with access to appropriate information.

As this Committee continues to explore the reauthorization of FCRA, I would like to stress the impact that this law has had on our ability to combat identity theft and help law enforcement officials track down illicit money under the PATRIOT Act. FCRA, and the information-sharing it has provided, is essential to protecting the American people by detecting suspicious activity and weeding out wrongdoers. The national uniform standards under FCRA have also facilitated a financial institution's ability to utilize additional authentications and identity verifications to protect consumer security. In addition, the protections incorporated in FCRA are critically important in enabling victims to correct the damage to their credit histories created by identity thieves.

Over the last few weeks, we have heard testimony from a diverse panel of witnesses endorsing the extension of FCRA's uniform standards. The Department of the Treasury specifically highlighted the importance of the national credit reporting system in helping to detect identity theft and in creating a framework for assisting its victims. I share these views and believe that we must reauthorize FCRA to protect Americans from these hideous and preventable crimes.

I thank the witnesses for appearing before the Committee. I look forward to working with you on strengthening our network to combat identity theft.

Testimony of
Joseph Ansanelli
Chairman and CEO of Vontu, Inc.

June 24, 2003
2128 Rayburn House Office Building
Washington, D.C.

Before the United States House of Representatives
Subcommittee on Financial Institutions and Consumer Credit
"Fighting Identity Theft – The Role of FCRA"

Introduction

My name is Joseph Ansanelli and I am the CEO and founder of Vontu. We provide information security software that guards against the loss of customer information. I am honored to provide testimony on fighting identity theft and the role of the Fair Credit Reporting Act. And I commend the Subcommittee members for discussing this important issue.

My testimony draws from my experience in working with Chief Information Security Officers at some of the country's top financial services, insurance, media and retail companies. These security professionals are acutely aware of the challenges in adequately protecting consumer information.

The Insider Security Threat

To begin, we believe it is important to help a consumer quickly repair his or her credit when their identity has been stolen. However, the problem will continue to grow if we do not prevent the theft of consumer data in the first place. While there are many ways identity theft occurs –a financial report stolen from the trash, a credit card receipt in a restaurant - companies and government agencies are the ultimate sources for large electronic databases

Vontu, Inc. 201 Spear Street | Suite 220 | San Francisco, CA 94105
415 227 8100 TEL 415 227 8190 FAX www.vontu.com WEB

of consumer information. Without additional safeguards in place, millions of Americans may be victims of identity theft by the end of this decade.

Traditionally, organizations have focused on the "hacker" and preventing break-ins to their customer data systems. Many organizations now realize that another significant threat exists. With the rapid adoption of the Internet and tools such as electronic mail, consumer information can be leaked in a moments notice by insiders. No matter how secure an organization's systems are, they must maintain many employees' access to sensitive customer data. Yet, it is much easier for employees to accidentally leak or maliciously steal information than it is for a thief to break in from the outside.

For example, in November 2002, a customer service employee of Teledata Communications Inc. who had easy access to consumer credit reports allegedly stole 30,000 customer records. This theft caused millions of dollars in financial losses and demonstrates that even though any computer system can be hacked, it is much easier, and in many cases far more damaging, for information to be stolen from the inside.

In May 2003, we conducted a survey with Harris Interactive of five hundred employees and managers with access to customer data. Almost half of the workers and managers said it would be "easy" to take sensitive customer information from their employers' network. Two-thirds believed their co-workers posed the greatest risk to consumer data security. Only ten percent said hackers were the biggest risk. It is important to look beyond external threats and recognize that insiders pose a fast growing risk.

Fighting Identity Theft and the Role of the Fair Credit Reporting Act

Based on my experience, I recommend the Subcommittee weigh the following when considering revisions to the Fair Credit Reporting Act.

Confusion is the Enemy of Consumer Protection

First, confusion is the enemy of consumer protection. A consistent and unified national approach to our credit system will benefit consumers the most. However well-intentioned a system of fifty different laws might be, it would only create confusion and paralysis that would ultimately harm consumer protection. Therefore, we believe that the preemption

provisions of the Fair Credit Reporting Act are critical and should extend to any additions to help protect against identity theft.

"Safe Harbor" for Best Practices

Second, we urge the Subcommittee to ensure that any modifications to the Fair Credit Reporting Act encourage companies to go above and beyond any stated requirements to protect consumers. Most companies know it is in their self interest to protect a customer's data. However, I have had companies question whether they should go beyond base legislative and regulatory requirements for fear in doing so could potentially reveal problems that trigger punitive actions. Future legislation should encourage and protect organizations that go beyond any base security requirements.

Consumer Data Security Standard

Third, I suggest this committee develop a Consumer Data Security standard as part of the Fair Credit Reporting Act. Ensuring a national, unified and standard approach to protecting consumer information will help to stop one of the main and growing sources of identity theft. Any such standard should include the following principles:

1. First, corporate security policies should be mandated. A company's security policies should be publicly available, regularly reviewed and updated, and audited and approved by its Board of Directors.

2. Second, employee education is critical. In the Harris survey I referenced earlier, almost one-third of workers and managers had not read or did not know if their company had a written consumer data security policy.

3. Third, data protection and control should require best practices. Physical and network protection should use best practices though all commercially reasonable solutions.

4. Fourth, companies must enforce employee compliance. Organizations should have an obligation to regularly monitor and enforce employee compliance with government regulations and internal security policies for the use and distribution of sensitive consumer information.

I hope these comments will prove helpful to the subcommittee as it continues its deliberations on the Fair Credit Reporting Act. I welcome the opportunity to continue working with you and am happy to answer any questions you might have.

Joseph Ansanelli
Chairman and Chief Executive Officer
Vontu, Inc.
(415) 227-8100

Consumer Data Security Survey Highlights

The following questions and responses are highlights of a survey of 500 U.S. workers and managers that handle sensitive customer information at work. The data for the survey was collected in May 2003 by Harris Interactive Service Bureau (HISB) and analyzed by Vontu.* Only workers and managers who said they have access to customer information were qualified to complete the survey.

- 62% reported incidents at work that could put customer data at risk for identity theft
- 66% say their co-workers, not hackers, pose the greatest risk to consumer privacy. Only 10% said hackers were the greatest threat.
- 70% say that government regulations play a role in raising awareness at their workplace about identity theft and database security
- Nearly 50% say government has still not done enough to help thwart identity theft.
- 46% say it would be "easy" to "extremely easy" for workers to remove sensitive data from the corporate database.
- 32%, about one in three, are unaware of internal company policies to protect customer data

Some of the more compelling questions and answers from the survey follow:

Does your company have a policy regulating what information is not okay to send out through email, Web mail, IM, etc.?

Yes 68.16%
No 14.56%
Not sure 17.26%

Have you read this policy in its entirety?

Yes 79.77%
No 20.23%

How would you characterize the level of security protecting customer information on your company's network?

Not at all secure 1.75%

Not very secure 5.44%

Somewhat secure 12.82%

Secure 19.61%

Very secure	27.77%
Extremely secure	26.41%
Not sure	6.21%

How easy would it be for someone at work to remove sensitive customer data from the corporate network?

Extremely difficult	10.87%
Very difficult	11.07%
Difficult	17.28%
Easy	25.44%
Very easy	11.07%
Extremely easy	8.54%
Not sure	15.73%

Which do you think poses the greatest threat to customer privacy and database security at your workplace?

Hackers who break into the network	10.49%
Workers at the company who abuse their access privileges	18.06%
Workers who have legitimate access to customer data	26.02%
A lack of understanding or education among workers	22.14%
I don't think there is any threat to customer privacy and data	23.30%

How do you access sensitive information that might include Social Security numbers, credit card numbers, account numbers or passwords? ***Please select all that apply.***

Web-based application	19.68%
Database application	62.76%
Documents	66.13%
Printouts	41.22%
Other	14.57%

Please indicate if you are aware of the following regulations.

- Gramm-Leach-Bliley Act or GLBA

  Yes 15.34%

  No 84.66%

- California SB1386

  Yes 5.24%

  No 94.76%

Now we'd like to ask some questions about your views on how involved the U.S. federal government should be in workplace issues.

Do you believe that government regulations encourage workers with access to sensitive information to be more aware of protecting that data?

Yes 67.83%

No 32.17%

Do current privacy regulations and policies help or hinder your efforts to protect sensitive information?

Help 35.38%

Hinder 10.22%

Neither 54.40%

On a scale of 1 to 5 with 1 not being enough and 5 being too much, please tell us if you believe the government has done enough to protect identity theft and customer data.

1	**Government has not done enough**	**25.02%**
2		**25.22%**
3		**34.70%**
4		**8.93%**
5	**Government has done too much**	**6.13%**

** Data for this survey were collected by the Harris Interactive Service Bureau (HISB) on behalf of Vontu. HISB was solely responsible for the quality of the online data collected and did not perform the survey design, data weighting or data analysis.*

PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION ON

IDENTITY THEFT: PREVENTION AND VICTIM ASSISTANCE

Before the

FINANCIAL INSTITUTIONS AND

CONSUMER CREDIT SUBCOMMITTEE

of the

HOUSE FINANCIAL SERVICES COMMITTEE

Washington, D.C.

June 24, 2003

I. INTRODUCTION

Mr. Chairman, and members of the Subcommittee, I am Howard Beales, Director of the Bureau of Consumer Protection, Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's views on the impact of identity theft on consumers and the importance of information security in preventing identity theft.

The Federal Trade Commission has a broad mandate to protect consumers, and controlling identity theft is an important issue of concern to all consumers. The FTC's primary role in combating identity theft derives from the 1998 Identity Theft Assumption and Deterrence Act ("the Identity Theft Act" or "the Act").[2] The Act directed the Federal Trade Commission to establish the federal government's central repository for identity theft complaints and to provide victim assistance and consumer education. The Commission also works extensively with industry on ways to improve victim assistance, including providing direct advice and assistance in cases when information has been compromised. The Commission can take enforcement action when companies fail to take adequate security precautions to protect consumers' personal information.

---

[1] The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily represent the views of the Commission or any Commissioner.

[2] Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028).

II. THE FEDERAL TRADE COMMISSION'S ROLE IN COMBATING IDENTITY THEFT

The Identity Theft Act strengthened the criminal laws governing identity theft[3] and focused on consumers as victims.[4] Congress also recognized that coordinated efforts are essential to best serve the needs of identity theft victims because these fraud victims often need assistance both from government agencies at the national and state or local level and from businesses. As a result, the FTC's role under the Act is primarily one of facilitating information sharing among public and private entities.[5] Specifically, Congress directed the Commission to establish procedures to: (1) log the receipt of complaints by victims of identity theft; (2) provide identity theft victims with

---

[3] 18 U.S.C. § 1028(a)(7). The statute broadly defines "means of identification" to include "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual," including, among other things, name, address, social security number, driver's license number, biometric data, access devices (*i.e.*, credit cards), electronic identification number or routing code, and telecommunication identifying information.

[4] Because individual consumers' financial liability is often limited, prior to the passage of the Act, financial institutions, rather than individuals, tended to be viewed as the primary victims of identity theft. Setting up an assistance process for consumer victims is consistent with one of the Act's stated goals: to recognize the individual victims of identity theft. *See* S. Rep. No. 105-274, at 4 (1998).

[5] Most identity theft cases are best addressed through criminal prosecution. The FTC itself has no direct criminal law enforcement authority. Under its civil law enforcement authority provided by Section 5 of the FTC Act, the Commission may, in appropriate cases, bring actions to stop practices that involve or facilitate identity theft. *See, e.g.*, FTC v. Assail, Inc., W03 CA 007 (W.D. Tex. Feb. 4, 2003) (order granting preliminary injunction) (defendants alleged to have debited consumers' bank accounts without authorization for "upsells" related to bogus credit card package) and FTC v. Corporate Marketing Solutions, Inc., CIV - 02 1256 PHX RCB (D. Ariz Feb. 3, 2003) (final order) (defendants "pretexted" personal information from consumers and engaged in unauthorized billing of consumers' credit cards). In addition, the FTC brought six complaints against marketers for purporting to sell international driver's permits that could be used to facilitate identity theft. Press Release, Federal Trade Commission, FTC Targets Sellers Who Deceptively Marketed International Driver's Permits over the Internet and via Spam (Jan. 16, 2003) (*at* http://www.ftc.gov/opa/2003/01/idpfinal.htm).

informational materials; and (3) refer complaints to appropriate entities, including the major national consumer reporting agencies and law enforcement agencies.[6] To fulfill the Act's mandate, the Commission has implemented a plan that focuses on three principal components: (1) A toll-free telephone hotline, (2) the Identity Theft Data Clearinghouse (the "Clearinghouse"), a centralized database used to aid law enforcement, and (3) outreach and education to consumers, law enforcement, and private industry.

A. Assisting Identity Theft Victims

The most immediate way in which the FTC assists victims is by collecting complaints and providing advice on recovery through a telephone hotline and a dedicated website. On November 1, 1999, the Commission began collecting complaints from consumers via a toll-free telephone number, 1-877-ID THEFT (438-4338). Every year since has seen an increase in complaints. In 2002, hotline counselors added almost 219,000 consumer records to the Clearinghouse, up from more than 117,000 in 2001. Of the 219,000 records, almost 162,000 (74%) were complaints from identity theft victims, and almost 57,000 (26%) were general inquiries about identity theft. Despite this dramatic growth in reports of identity theft, the FTC is cautious in attributing it entirely to a commensurate growth in the prevalence of identity theft. The FTC believes that the increase is, at least in part, an indication of successful outreach in informing the public of its program and the availability of assistance.

Callers to the hotline receive telephone counseling from specially trained personnel who provide general information about identity theft and help guide victims through the steps needed to resolve the problems resulting from the misuse of their identities. Victims are advised to: (1)

---

[6] Pub. L. No. 105-318, § 5, 112 Stat. 3010 (1998).

place a fraud alert on their credit reports and review their credit reports for additional fraudulent accounts;[7] (2) contact each of the creditors or service providers where the identity thief has established or accessed an account, to request that the account be closed and to dispute any associated charges; and (3) report the identity theft to the police and get a police report, which is very helpful in demonstrating to would-be creditors and debt collectors that the consumers are genuine victims of identity theft.

Counselors also advise victims having particular problems about their rights under relevant consumer credit laws including the Fair Credit Reporting Act,[8] the Fair Credit Billing Act,[9] the Truth in Lending Act,[10] and the Fair Debt Collection Practices Act.[11] If the investigation and resolution of the identity theft falls under the jurisdiction of another regulatory agency that has a program in place to assist consumers, callers also are referred to those agencies.

The FTC's identity theft website, located at www.consumer.gov/idtheft, provides equivalent service for those who prefer the immediacy of an online interaction. The site contains a secure complaint form, which allows victims to enter their identity theft information for input into

---

[7] At a consumer's request, the three major credit reporting agencies will place a fraud alert on the consumer's credit file that indicates to credit issuers that the consumer is to be contacted before new credit is issued in that consumer's name. *See* Section II.B.(3)(a) *infra* for a discussion of the credit reporting agencies new "joint fraud alert" initiative.

[8] 15 U.S.C. § 1681 *et seq.*

[9] *Id.* § 1666. The Fair Credit Billing Act generally applies to "open end" credit accounts, such as credit cards, revolving charge accounts, and overdraft checking accounts. It does not cover installment contracts, such as loans or extensions of credit that are repaid on a fixed schedule.

[10] *Id.* § 1601 *et seq.*

[11] *Id.* § 1692 *et seq.*

the Clearinghouse. Victims also can read and download all of the resources necessary for reclaiming their credit record and good name. One resource in particular is the FTC's tremendously successful consumer education booklet, *Identity Theft: When Bad Things Happen to Your Good Name*. The 26-page booklet, now in its fourth edition, comprehensively covers a range of topics, including the first steps to take for victims, how to correct credit-related and other problems that may result from identity theft, tips for those having trouble getting a police report taken, and advice on ways to protect personal information. It also describes federal and state resources that are available to victims who may be having particular problems as a result of the identity theft. The FTC alone has distributed more than 1.2 million copies of the booklet since its release in February 2000.[12] Last year, the FTC released a Spanish language version of the Identity Theft booklet, *Robo de Identidad: Algo malo puede pasarle a su buen nombre.*

B. Outreach and Education

The Identity Theft Act also directed the FTC to provide information to consumers about identity theft. Recognizing that law enforcement and private industry play an important part in the ability of consumers both to minimize their risk and to recover from identity theft, the FTC expanded its mission of outreach and education to include these sectors.

(1) *Consumers*: The FTC has taken the lead in coordinating with other government agencies and organizations in the development and dissemination of comprehensive consumer education materials for victims of identity theft and those concerned with preventing this crime. The FTC's extensive consumer and business education campaign includes print materials, media

---

[12] Other government agencies, including the Social Security Administration, the SEC, and the FDIC also have printed and distributed copies of *Identity Theft: When Bad Things Happen to Your Good Name.*

mailings, and radio and television interviews. The FTC also maintains the identity theft website, which includes the publications and links to testimony, reports, press releases, identity theft-related state laws, and other resources.

To increase identity theft awareness for the average consumer, the FTC recently developed a new primer on identity theft, *ID Theft: What's It All About?* This publication discusses the common methods of identity thieves, how consumers can best minimize their risk of being victimized, how to identify the signs of victimization, and the basic first steps for victims. Taken together with the detailed victim recovery guide, *Identity Theft: When Bad Things Happen to Your Good Name*, the two publications help to fully educate consumers.

(2) *Law Enforcement*: Because law enforcement at the state and local level can provide significant practical assistance to victims, the FTC places a premium on outreach to such agencies. In addition to the training described below (*see infra* Section II.C.), the staff joined with North Carolina's Attorney General Roy Cooper to send letters to every other Attorney General letting him or her know about the FTC's identity theft program and how each Attorney General could use the resources of the program to better assist residents of his or her state. The letter encourages the Attorney General to link to the consumer information and complaint form on the FTC's website and to let residents know about the hotline, stresses the importance of the Clearinghouse as a central database, and describes all of the educational materials that the Attorney General can distribute to residents. North Carolina took the lead in availing itself of the Commission's resources in putting together for its resident victims a package of assistance that includes the ID Theft Affidavit (*see* Section II.B.(3)(a)) and links to the FTC website, www.consumer.gov/idtheft. Through this initiative, the FTC hopes to make the most efficient use

of federal resources by allowing states to take advantage of the work the FTC has already accomplished and at the same time continuing to expand the centralized database of victim complaints and increase its use by law enforcement nationwide. Other outreach initiatives include: (1) Participation in a "Roll Call" video produced by the Secret Service, which will be sent to thousands of law enforcement departments across the country to instruct officers on identity theft, investigative resources, and assisting victims; and (2) redesigning of the FTC's website to include a section for law enforcement with tips on how to help victims as well as resources for investigations. The FTC will launch the new website this summer.

(3) *Industry*:

(a) Victim Assistance: Identity theft victims spend significant time and effort restoring their good name and financial records. As a result, the FTC devotes significant resources to conducting outreach with the private sector on ways to improve victim assistance procedures. One such initiative arose from the burdensome requirement that victims complete a different fraud affidavit for each different creditor with whom the identity thief had opened an account.[13] To reduce that burden, the FTC worked with industry and consumer advocates to create a standard form for victims to use in resolving identity theft debts. From its release in August 2001 through April 2003, the FTC has distributed more than 293,000 print copies of the ID Theft Affidavit. There have also been more than 356,000 hits to the Web version. The affidavit is available in both English and Spanish.

---

[13] *See ID Theft: When Bad Things Happen to Your Good Name: Hearing Before the Subcomm. on Technology, Terrorism and Government Information of the Senate Judiciary Comm.* 106th Cong. (2000) (statement of Mrs. Maureen Mitchell, Identity Theft Victim).

The three major credit reporting agencies ("CRAs") recently launched a new initiative, the "joint fraud alert." After receiving a request from an identity theft victim for the placement of a fraud alert on his or her consumer report and for a copy of that report, each CRA now shares that request with the other two CRAs, thereby eliminating the requirement that the victim contact each of the three major CRAs separately.

(b) Information Security Breaches: Additionally, the FTC is working with institutions that maintain personal information to identify ways to help keep that information safe from identity theft. Last year, the FTC invited representatives from financial institutions, credit issuers, universities, and retailers to an informal roundtable discussion of how to prevent unauthorized access to personal information in employee and customer records. The FTC will soon publish a self-assessment guide to make businesses and organizations of all sizes more aware of how they manage personal information and to aid them in assessing their security protocols.

As awareness of the FTC's role in identity theft has grown, businesses and organizations that have suffered compromises of personal information have begun to contact the FTC for assistance. For example, in the cases of TriWest[14] and Ford/Experian,[15] in which tens of thousands of consumers' files were compromised, the Commission advised how to notify those individuals and how to protect the data in the future. To provide better assistance in these types of cases, the FTC developed a kit, *Responding to a Theft of Customer or Employee Information*, that will be posted on the identity theft website in the coming weeks. The kit provides advice on which

---

[14] Adam Clymer, *Officials Say Troops Risk Identity Theft After Burglary*, N.Y. TIMES, Jan. 12, 2003, § 1 (Late Edition), at 12.

[15] Kathy M. Kristof and John J. Goldman, *3 Charged in Identity Theft Case*, LA TIMES, Nov. 6, 2002, Main News, Part 1 (Home Edition), at 1.

law enforcement agency to contact, depending on the type of compromise, business contact information for the three major credit reporting agencies, suggestions for establishing an internal communication protocol, information about contacting the FTC for assistance, and a detailed explanation of what information individuals need to know. The kit also includes a form letter for notifying the individuals whose information was taken. Organizations are encouraged to print and include copies of *Identity Theft: When Bad Things Happen to Your Good Name* with the letter to individuals.

The FTC particularly stresses the importance of notifying individuals as soon as possible when information has been taken that may put them at risk for identity theft. They can then begin to take steps to limit the potential damage to themselves. Individuals who place a fraud alert promptly have a good chance of preventing, or at least reducing, the likelihood that the release of their information will turn into actual misuse. Prompt notification also alerts these individuals to review their credit reports and to watch for the signs of identity theft. In the event that they should become victims, they can quickly take action to clear their records before any long-term damage is done. Besides providing *Responding to a Theft of Customer or Employee Information*, FTC staff can provide individual assistance and advice, including review of consumer information materials for the organization and coordination of searches of the Clearinghouse for complaints with the law enforcement officer working the case.

C. Identity Theft Data Clearinghouse

The final mandate for the FTC under the Identity Theft Act was to log the complaints from victims of identity theft and refer those complaints to appropriate entities such as law enforcement agencies. Before launching this complaint system, the Commission took a number of steps to ensure that it would meet the needs of criminal law enforcement, including meeting with a host of law enforcement and regulatory agencies to obtain feedback on what the database should contain. Access to the Clearinghouse via the FTC's secure Web site became available in July of 2000. To ensure that the database operates as a national clearinghouse for complaints, the FTC has solicited complaints from other sources. For example, in February 2001, the Social Security Administration Office of Inspector General (SSA-OIG) began providing the FTC with complaints from its fraud hotline, significantly enriching the FTC's database.

The Clearinghouse provides a much fuller picture of the nature, prevalence, and trends of identity theft than was previously available.[16] FTC data analysts aggregate the data to develop statistics about the nature and frequency of identity theft. For instance, the Commission publishes charts showing the prevalence of identity theft by states and by cities. Law enforcement and policy makers at all levels of government use these reports to better understand the challenges identity theft presents.

Since the inception of the Clearinghouse, 62 federal agencies and 574 state and local agencies have signed up for access to the database. Within those agencies, over 4,200 individual

---

[16] Charts that summarize 2002 data from the Clearinghouse can be found at www.consumer.gov/idtheft and www.consumer.gov/sentinel.

investigators have the ability to access the system from their desktop computers twenty-four hours a day, seven days a week. The Commission actively encourages even greater participation.

One of the goals of the Clearinghouse and the FTC's identity theft program is to provide support for identity theft prosecutions nationwide.[17] Last year, in an effort to further expand the use of the Clearinghouse among law enforcement, the FTC, in cooperation with the Department of Justice, the International Association of Chiefs of Police and the United States Secret Service, initiated a full day identity theft training seminar for state and local law enforcement officers. Sessions were held in Washington, D.C., Des Moines, Chicago, San Francisco, Las Vegas, Dallas, and Phoenix. The Phoenix program was held May 22. More than 730 officers have attended these seminars, representing more than 170 different agencies. Additional training seminars will occur later this year in Seattle, New York, and Houston -- cities the FTC has identified as having high rates of identity theft. Also, the FTC is a member of an identity theft task force in Kansas City and is helping coordinate a training seminar there later this summer.

The FTC staff also helps develop case leads. Now in its second year, the Commission runs an identity theft case referral program in coordination with the United States Secret Service. The Secret Service has assigned a special agent on a full-time basis to the Commission to assist with identity theft issues and has provided the services of its Criminal Research Specialists.[18]

---

[17] The Commission testified last year in support of S. 2541, the Identity Theft Penalty Enhancement Act of 2002, which would increase penalties and streamline proof requirements for prosecution of many of the most harmful forms of identity theft. *See* Testimony of Bureau Director J. Howard Beales, Senate Judiciary Committee, Subcommittee on Terrorism, Technology and Government Information (July 11, 2002). S. 2541 has been reintroduced in the 108th Congress as S. 153.

[18] The referral program complements the regular use of the database by all law (continued...)

Together, the FTC and Secret Service staff develop preliminary investigative reports by examining significant patterns of identity theft activity in the database and refining the data through the use of additional investigative resources. Thereupon, the staff refer the investigative reports to appropriate Financial Crimes Task Forces and other law enforcers located throughout the country for further investigation and potential prosecution.

III. CONCLUSION

Identity theft places substantial costs on individuals and businesses. The Commission, through its education and enforcement capabilities, is committed to reducing these breaches as much as possible. The Commission will continue its efforts to assist criminal law enforcement with their investigations. Prosecuting perpetrators sends the message that identity theft is not cost-free. Finally, the Commission knows that as with any crime, identity theft can never be completely eradicated. Thus, the Commission's program to assist victims and work with the private sector on ways to facilitate the process for regaining victims' good names will always remain a priority.

---

[18] (...continued)
enforcers from their desk top computers.

Statement of Mr. Timothy Caddigan

Special Agent in Charge
Criminal Investigative Division
United States Secret Service

Presentation to the House Subcommittee on Financial Institutions and Consumer Credit

Committee on Financial Services

U.S. House of Representatives

June 24, 2003

Mr. Chairman, Mr. Sanders, thank you for inviting me to be part of this hearing today, and the opportunity to address the subcommittee regarding the Secret Service's efforts to combat identity crime and protect our nation's financial infrastructure.

The Secret Service was originally established within the Department of the Treasury in 1865 to combat the counterfeiting of U.S. currency. Since that time, this agency has been tasked with the investigation of financial crimes, as well as the protection of our nation's leaders, visiting foreign dignitaries and events of national significance. Although we have moved to the Department of Homeland Security, the Secret Service has maintained historic relationships with the Department of the Treasury in our ongoing efforts to ensure a secure financial services infrastructure.

With the passage of new federal laws in 1982 and 1984, the Secret Service was provided primary authority for the investigation of access device fraud, including credit and debit card fraud, and parallel authority with other law enforcement agencies in identity crime cases. The explosive growth of these crimes has resulted in the evolution of the Secret Service into an agency that is recognized worldwide for its expertise in the investigation of all types of financial crimes. Our efforts to detect, investigate and prevent financial crimes are aggressive, innovative and comprehensive.

The burgeoning use of the Internet and advanced technology, coupled with increased investment and expansion, has intensified competition within the financial sector. With lower costs of information-processing, legitimate companies have found it profitable to specialize in data mining, data warehousing and information brokerage. Information collection has become a common byproduct of newly-emerging e-commerce. Internet purchases, credit card sales, and other forms of electronic transactions are being captured, stored, and analyzed by businesses seeking to find the best customers for their products.

This has led to a new measure of growth within the direct marketing industry that promotes the buying and selling of personal information. In today's markets, consumers routinely provide personal and financial identifiers to companies engaged in business on the Internet. They may not realize that the information they provide in credit card applications, loan applications, or with merchants they patronize are valuable commodities in this new age of information trading. Consumers may be even less aware of the illegitimate uses to which this information can be put. This wealth of available personal information creates a target-rich environment for today's sophisticated criminals, many of whom are organized and operate across international borders. But legitimate business can provide a first line of defense against identity crime by safeguarding the information it collects. Such efforts can significantly limit the opportunities for identity crime, even while not eliminating its occurrence altogether.

Simply stated, identity crime is the theft or misuse of an individual's personal or financial identifiers in order to gain something of value or to facilitate other criminal activity. Types of identity crime include identity theft, credit card fraud, bank fraud, check fraud, false identification fraud, and passport/visa fraud. Identity crimes are almost always associated with other crimes such as narcotics and weapons trafficking, organized crime, mail theft and fraud, money laundering, immigration fraud, and terrorism.

According to statistics compiled by the FTC for the year 2002, 22% of the 161,819 victim complaints reported involved more than one type of identity crime. The complaints were broken down as follows (note that some complaints involved more than one of the listed activities):

- **42%** of complaints involved credit card fraud – i.e. someone either opened up a credit card account in the victim's name or "took over" their existing credit card account;
- **22%** of complaints involved the activation of telephone, cellular, or other utility service in the victim's name;
- **17%** of complaints involved bank accounts that had been opened in the victim's name, and/or fraudulent checks had been negotiated in the victim's name;
- **9%** of complaints involved employment-related fraud;
- **8%** of complaints involved government documents/benefits fraud;
- **6%** of complaints involved consumer loans or mortgages that were obtained in the victim's name; and
- **16%** of complaints involved some type of miscellaneous fraud, such as medical, bankruptcy and securities fraud.

Identity crime is not targeted against any particular demographic; instead, it affects all types of Americans, regardless of age, gender, nationality, or race. Victims include

everyone from restaurant workers, telephone repair technicians and police officers, to corporate and government executives, celebrities and high-ranking military officers. What victims do have in common is the difficult, time consuming, and potentially expensive task of repairing the damage that has been done to their credit, their savings, and their reputation. According to a report by the General Accounting Office, the average victim spends over 175 hours attempting to repair the damage done by identity criminals.

In past years, victims of financial crimes such as bank fraud or credit card fraud were identified by statute as the person, business, or financial institution that incurred a financial loss. All too often the individuals whose credit was ruined through identity theft were not even recognized as victims. As a result of the passage of the Identity Theft and Assumption Deterrence Act in 1998, this is no longer the case. This legislation represented the first comprehensive effort to re-write the federal criminal code to address the insidious affects of identity theft on private citizens. This new law amended Section 1028 of Title 18 of the United States Code to provide enhanced investigative authority to combat the growing problem of identity theft. These protections included:

- The establishment of the Federal Trade Commission (FTC) as the central clearinghouse for victims to report incidents of identity theft. This centralization of all identity theft cases allows for the identification of systemic weaknesses and provides law enforcement with the ability to retrieve investigative data at one central location. It further allows the FTC to provide victims with the information and assistance they need in order to take the steps necessary to correct their credit records;

- The enhancement of asset forfeiture provisions to allow for the repatriation of funds to victims; and

- The closing of a significant gap in then-existing statutes. Previously, only the production or possession of false identification documents was unlawful. However, with advances in technology such as E-commerce and the Internet, criminals did not need actual, physical identification documents to assume an identity. This statutory change made it illegal to steal another person's personal identification *information* with the intent to commit a violation, regardless of actual possession of identity *documents*.

We believe that the passage of this legislation was the catalyst needed to bring together both federal and state government resources in a focused and unified response to the identity crime problem. Today, law enforcement, regulatory and community assistance organizations have joined forces through a variety of working groups, task forces, and information sharing initiatives to assist victims of identity crime.

As you know, Mr. Chairman, the Senate recently passed the Identity Theft Penalty Enhancement Act of 2002. The intent of this act is to establish increased penalties for aggravated identity theft -- that is, identity theft committed during and in relation to certain specified felonies. This act, in part, provides for two years imprisonment for the

identity crime, in addition to the punishment associated with the related felony and five years imprisonment if the related felony is associated with terrorism. Additionally, the Act prohibits the imposition of probation and allows for consecutive sentences. While this particular legislation cannot be expected to completely suppress identity theft, it does recognize the impact identity theft has on consumers and the need to punish those engaging in criminal activity for personal or financial gain. The Secret Service supports these ideas and believes they represent additional tools that law enforcement can utilize to the fullest extent in protecting the American people.

Identity crime violations are investigated by federal law enforcement agencies, including the Secret Service, the U.S. Postal Inspection Service, the Social Security Administration (Office of the Inspector General), and the Federal Bureau of Investigation. Schemes to commit identity crime may also involve violations of other statutes, such as computer crime, mail theft and fraud, wire fraud, or Social Security fraud, as well as violations of state law. Because most identity crimes fall under the jurisdiction of the Secret Service, we have taken an aggressive stance and continue to be a leading agency for the investigation and prosecution of such criminal activity.

Although financial crimes are often referred to as "white collar" by some, this characterization can be misleading. The perpetrators of such crimes are increasingly diverse and today include both domestic and international organized criminal groups, street gangs, convicted felons and terrorists.

The personal identifiers most often sought by criminals are those generally required to obtain goods and services on credit. These are primarily social security numbers, names, and dates of birth. Identity crimes also involve the theft or misuse of an individual's financial identifiers such as credit card numbers, bank account numbers and personal identification numbers.

The methods of identity criminals vary. It has been determined that many "low tech" identity criminals obtain personal and financial identifiers by going through commercial and residential trash, a practice known as "dumpster diving." The theft of both incoming and outgoing mail is a widespread practice employed by both individuals and organized groups, along with thefts of wallets and purses.

With the proliferation of computers and increased use of the Internet, many identity criminals have used information obtained from company databases and web sites. A case investigated by the Secret Services that illustrates this method involved an identity criminal accessing public documents to obtain the social security numbers of military officers. In some cases, the information obtained is in the public domain while in others it is proprietary and is obtained by means of a computer intrusion.

The method that may be most difficult to prevent is theft by a collusive employee. The Secret Service has discovered that individuals or groups who wish to obtain personal or financial identifiers for a large-scale fraud ring will often pay or extort an employee who

has access to this information through their employment at workplaces such as a financial institution, medical office, or government agency.

In most of the cases that our agency has investigated involving identity theft, criminals have used an individual's personal identifiers to apply for credit cards or consumer loans. Additionally, these identifiers were also used to establish bank accounts, leading to the laundering of stolen or counterfeit checks or were used in a check-kiting scheme.

The majority of identity crime cases investigated by the Secret Service are initiated on the local law enforcement level. In most cases, the local police department is the first responder to the victims once they become aware that their personal or financial identifiers are being used unlawfully. Credit card issuers as well as financial institutions will also contact a local Secret Service field office to report possible criminal activity.

The events of September 11, 2001 have altered the priorities and actions of law enforcement throughout the world, including the Secret Service. Immediately following the attacks, Secret Service assisted the FBI with their terrorism investigation through the leveraging of our established relationships, especially within the financial sector, in an attempt to gather information as expeditiously as possible.

As part of the new Department of Homeland Security, the Secret Service will continue to be involved in a collaborative effort with the intention of analyzing the potential for identity crime to be used in conjunction with terrorist activities through our liaison efforts with the Bureau of Immigration and Customs Enforcement, Operation Direct Action, FinCEN, the Diplomatic Security Service and the Terrorist Financing Operations Section of the FBI.

The Secret Service continues to attack identity crime by aggressively pursuing our core Title 18 investigative violations, including access and telecommunications device fraud, financial institution fraud, computer fraud and counterfeiting. Many of these schemes are interconnected and depend upon stealing and misusing the personal and financial identifiers of innocent victims.

Our own investigations have frequently involved the targeting of organized criminal groups that are engaged in financial crimes on both a national and international scale. Many of these groups are prolific in their use of stolen financial and personal identifiers to further their other criminal activity.

It has been our experience that the criminal groups involved in these types of crimes routinely operate in a multi-jurisdictional environment. This has created problems for local law enforcement agencies that generally act as the first responders to their criminal activities. By working closely with other federal, state, and local law enforcement, as well as international police agencies, we are able to provide a comprehensive network of intelligence sharing, resource sharing, and technical expertise that bridges jurisdictional boundaries. This partnership approach to law enforcement is exemplified by our financial and electronic crime task forces located throughout the country, pursuant to our

section 1030 computer crime authority. These task forces primarily target suspects and organized criminal enterprises engaged in financial and electronic criminal activity that falls within the investigative jurisdiction of the Secret Service. Members of these task forces, who include representatives from local and state law enforcement, prosecutors offices, private industry and academia, pool their resources and expertise in a collaborative effort to detect and prevent electronic crimes. The value of this crime fighting and crime prevention model has been recognized by Congress, which has authorized the Secret Service (pursuant to the USA/Patriot Act of 2001) to expand our electronic crime task forces to cities and regions across the country. Recently, four new Electronic Crimes Task Forces were established in Dallas, Houston, Columbia (SC) and Cleveland, bringing the total number of ECTFs to 13.

While our task forces do not focus exclusively on identity crime, we recognize that stolen identifiers are often a central component of other electronic or financial crimes. Consequently, our task forces devote considerable time and resources to the issue of identity crime.

Another important component of the Secret Service's preventative and investigative efforts has been to increase awareness of issues related to financial crime investigations in general, and of identity crime specifically, both in the law enforcement community and the general public. The Secret Service has tried to educate consumers and provide training to law enforcement personnel through a variety of partnerships and initiatives.

For example, criminals increasingly employ technology as a means of communication, a tool for theft and extortion, and a repository for incriminating information. As a result, the investigation of all types of criminal activity, including identity crime, now routinely involves the seizure and analysis of electronic evidence. In fact, so critical was the need for basic training in this regard that the Secret Service joined forces with the International Association of Chiefs of Police and the National Institute for Justice to create the "Best Practices Guide to Searching and Seizing Electronic Evidence" which is designed for the first responder, line officer and detective alike. This guide assists law enforcement officers in recognizing, protecting, seizing and searching electronic devices in accordance with applicable statutes and policies.

We have also worked with these same partners in producing the interactive, computer-based training program known as "*Forward Edge*," which takes the next step in training officers to conduct electronic crime investigations. *Forward Edge* is a CD-ROM that incorporates virtual reality features as it presents three different investigative scenarios to the trainee. It also provides investigative options and technical support to develop the case. Copies of state computer crime laws for each of the fifty states as well as corresponding sample affidavits are also part of the training program and are immediately accessible for instant implementation.

Thus far, we have distributed over 300,000 "Best Practices Guides" to local and federal law enforcement officers and have distributed, free of charge, over 20,000 *Forward Edge* training CDs.

In April of 2001, the Secret Service assisted the FTC in the design of an identity theft brochure, containing information to assist victims on how to restore their "good name", as well as how to prevent their information and identities from becoming compromised.

In addition, we have just completed the Identity Crime Video/CD-ROM which contains over 50 investigative and victim assistance resources that local and state law enforcement officers can use when combating identity crime. This CD-ROM also contains a short identity crime video that can be shown to police officers at their roll call meetings which discusses why identity crime is important, what other departments are doing to combat identity crime, and what tools and resources are available to officers. The Identity Crime CD-ROM is an interactive resource guide that was made in collaboration with the U.S. Postal Inspection Service, the Federal Trade Commission and the International Association of Chiefs of Police.

Next week, we will be sending an Identity Crime CD-ROM to every law enforcement agency in the United States. Departments can make as many copies of the CD-ROM as they wish and distribute this resource to their officers to use in identity crime investigations. Over 25,000 Identity Crime CD-ROMs have been produced and are being prepared for distribution.

The Secret Service is also actively involved with a number of government-sponsored initiatives. At the request of the Attorney General, the Secret Service joined an interagency identity theft subcommittee that was established by the Department of Justice. This group, which is comprised of federal, state, and local law enforcement agencies, regulatory agencies, and professional agencies, meets regularly to discuss and coordinate investigative and prosecutive strategies as well as consumer education programs.

In a joint effort with the Department of Justice, the U.S. Postal Inspection Service, the Federal Trade Commission and the International Association of Chiefs of Police, we are hosting Identity Crime Training Seminars for law enforcement officers. In the last year and a half we have held seminars for officers in Chicago, Dallas, Las Vegas, Iowa, Washington D.C., and Phoenix. In the coming months we have training seminars scheduled in New York, Seattle and Texas. These training seminars are focused on providing local and state law enforcement officers with tools and resources that they can immediately put into use in their investigations of identity crime. Additionally, officers are provided resources that they can pass on to members of their community who are victims of identity crime.

The Secret Service's Criminal Investigative Division assigned a special agent to the Federal Trade Commission (FTC) as a liaison to support all aspects of their program to encourage the use of the Identity Theft Data Clearinghouse as a law enforcement tool. The FTC has done an excellent job of providing people with the information and assistance they need in order to take the steps necessary to correct their credit records, as well as undertaking a variety of "consumer awareness" initiatives regarding identity theft.

It is important to recognize that public education efforts can only go so far in combating the growth of identity crime. Because social security numbers, in conjunction with other personal and financial identifiers, are used for such a wide variety of record keeping and credit related applications, even a consumer who takes appropriate precautions to safeguard such information is not immune from becoming a victim.

The Secret Service recommends that consumers take the following steps to protect themselves from identity crime:

- Maintain a list of all credit card accounts and corresponding phone numbers. Keep this list in a place other than your wallet or purse so that immediate notification can occur if any cards are lost or stolen;
- Avoid carrying any more credit cards in a wallet or purse than is actually needed;
- Cancel any accounts that are not in use;
- Be conscious of when billing statements should be received, and if they are not received during that window, contact the sender;
- Check credit card bills against receipts before paying them;
- Avoid using a date of birth, social security number, name or similar information as a password or PIN code, and change passwords at least once a year;
- Shred or burn pre-approved credit card applications, credit card receipts, bills and other financial information that you do not want to save;
- Secure your incoming and outgoing mail;
- Establish passwords where possible with credit card companies or financial institutions that you have accounts with in order to avoid unauthorized change of address, transfer of funds or orders of additional cards;
- Order a credit report once a year from each of the three major credit bureaus to check for inaccuracies and fraudulent use of accounts; and
- Avoid providing any personal information over the telephone unless you initiated the call, and be aware that individuals and business contacted via the Internet may misrepresent themselves.

Should an individual become the victim of identity theft, the Secret Service recommends the following steps:

- Report the crime to the police immediately and get a copy of the police report;

- Immediately notify your credit card issuers and request replacement cards with new account numbers. Also, request that the old account be processed as "account closed at consumers' request" for credit record purposes. Ask that a password be used before any inquiries or changes can be made on the new account. Follow up the telephone conversation with a letter summarizing your requests;

- Call the fraud units of the three credit reporting bureaus, and report the theft of your credit cards and/or numbers. Ask that your accounts be flagged, and add a victim's statement to your report that requests that they contact you to verify future credit applications. Order copies of your credit reports so you can review them to make sure no additional fraudulent accounts have been opened in your name;

- File a complaint with the Federal Trade Commission (FTC) by calling 1-877-ID-THEFT or writing to them at Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave NW, Washington, DC 20580. Complaints can also be filed via their website at www.ftc.gov/ftc/complaint.htm; and

- Follow up with the credit bureaus every three months for at least a year and order new copies of your reports so that you can verify that corrections have been made, and to make sure that no new fraudulent accounts have been established.

CONCLUSION

For law enforcement to properly prevent and combat identity crime, steps must be taken to ensure that local, state and federal agencies are addressing victim concerns in a consistent manner. All levels of law enforcement should be familiar with the resources available to combat identity crime and to assist victims in rectifying damage inflicted on their credit. It is essential that law enforcement recognize that identity crimes must be combated on all fronts, from the officer who receives a victim's complaint, to the detective or Special Agent investigating an organized identity crime ring.

The Secret Service has already launched a number of initiatives aimed at increasing awareness and providing the training necessary to address these issues, but those of us in the law enforcement and consumer protection communities need to continue to reach out to an even larger audience. We need to continue to approach these investigations with a coordinated effort – this is central to providing a consistent level of vigilance and addressing investigations that are multi-jurisdictional while avoiding duplication of effort. The Secret Service is prepared to assist this committee in protecting and assisting the people of the United States, with respect to the prevention, identification and prosecution of identity criminals.

Mr. Chairman, that concludes my prepared remarks and I would be happy to answer any questions that you or other members of the subcommittee may have.

Testimony of

Janell Mayo Duncan

Legislative and Regulatory Counsel

Consumers Union

On

"Fighting Identity Theft -- The Role of FCRA"

Before the

House Financial Services

Subcommittee on Financial Institutions and Consumer Credit

June 24, 2003

Good morning, Chairman Bachus, Ranking Member Sanders, and Members of the Subcommittee. Thank you for providing me the opportunity to come before you today. I am Janell Mayo Duncan, Legislative and Regulatory Counsel for Consumers Union.[1] Consumers Union is the nonprofit publisher of *Consumer Reports* magazine. Our mission at Consumers Union is to test products, inform the public, and protect consumers. Today I offer this testimony on Identity Theft and its relationship to the Fair Credit Reporting Act as part of our consumer protection function.

Identity theft presents an alarming crisis in the United States. Between 2000 and 2002, the Federal Trade Commission (FTC) reported that Identity theft had topped the list of complaints received from consumers. In fact, of the 218,714 reports the FTC processed through its Identity Theft Clearinghouse in 2002, 74% were from victims of identity theft. Although these numbers are high, they represent only those consumers reporting to FTC, and may represent only a fraction of the total number of people victimized last year.

Types of Fraud

Identity theft occurs when a criminal obtains identifying information, usually a person's name or social security number, and begins to represent him or herself as that person. In this electronic age, a thief can obtain an individual's personal information without physically stealing either a wallet or mail. For example, a growing number of cases involve "inside jobs," where employees have or gain access to consumer information in their workplace. Once a thief has the consumer's personal identifiers, he can engage in a number of fraudulent activities, such as

[1] Consumers Union is a nonprofit membership organization chartered in 1936 under the laws of the State of New York to provide consumers with information, education and counsel about goods, services, health, and personal finance. Consumers Union's income is solely derived from the sale of *Consumer Reports*, its other publications and from noncommercial contributions, grants and fees. In addition to reports on Consumers Union's own product testing, *Consumer Reports* with approximately 4.5 million paid circulation, regularly carries articles on health, product safety, marketplace economics and legislative, judicial and regulatory actions that affect consumer welfare. Consumers Union's publications carry no advertising and receive no commercial support.

taking over a consumer's existing account or applying for new lines of credit in the victim's name.

The victim may not become aware that they have been victimized for months. According to a May 2000 victim survey conducted by the California Public Interest Research Group (CALPIRG), the average victim did not know what had occurred for 14 months. Once aware of the problem, according to the FTC, CALPIRG and the Privacy Rights Clearinghouse, in addition to suffering stress and aggravation, the average victim spends 175 hours and $808 seeking to remedy the situation. Even worse, according to a March 2002 GAO Report, 1,300 consumers reporting harm suffered to the FTC Identity Theft Clearinghouse between November 1999 and September 2001 said they had been wrongfully investigated, arrested, or convicted due to the criminal acts of an identity thief.

Industry Practices

The September 1997 issue of Consumer Reports Magazine included an article entitled, "Are you a target for identity theft?" The article described the crime as "one of the fastest growing in the nation," and chronicled, among other victims, the experience of Adelaide Andrews, whose identity was co-opted by a thief in 1995. (The September Consumer Reports Article is attached to my testimony).

Six years after the article, consumers continue to be victimized by identity theft. The similarity of victims' stories today evidences continuing industry practices that make committing these crimes possible. In the article, we expressed concern at flaws in the credit granting system, and identified several factors that contributed to the occurrence of identity theft, including:

- **Lax identification verification standards.** Where "[t]he credit approval process often amounts to little more than matching two bits of information on the application

-- name and Social Security Number -- with the same information of the credit report of anyone with a good credit score." (Consumer Reports, September 1997, at 13);

- **Too-convenient credit.** The granting of "quick credit," and practices that have been exploited by criminals such as the dissemination of convenience checks, and careless provision of replacement cards for lost or stolen credit cards;
- **Carelessness with credit files.** A consumer credit report can be obtained from Credit Reporting Agencies (CRAs) with only a victim's name and social security number. A thief with only these two pieces of information, and even sometimes with a name and address alone, can therefore easily apply for credit in an unwitting victim's name.[2] In addition, the credit reporting system will automatically change the consumer's file to include the address of the thief after credit is applied for in the victim's name, thereby making it harder for a victim to discover the crime;
- **Inadequate fraud detection.** At the time the article was published, credit bureaus did not monitor for changes in the normal patterns -- however, they now will do so, but only after charging the consumer a fee;
- **Ignored fraud warnings.** Creditors are so eager to lend money that they ignore fraud alerts a consumer has put on his or her file and grant credit to imposters anyway; and
- **Unfair correction practices.** Credit bureaus updating files with inaccurate information, requiring consumers to repeatedly prove their innocence -- sometimes for years.

[2]More recently it has become evident that CRAs may disclose a credit report in response to a credit application even when a Social Security Number is not submitted.

We believe that curbing the incidence of this crime will require getting ahead of problem.[3] The last portion of my testimony contains recommendations that appeared in the 1997 article, as well as additional recommendations for ways to protect consumers from this crime.

Less, Not More, Sharing of Consumer Information is Needed

Some members of industry claim that the key to solving identity theft is to allow unfettered sharing of consumers' personal financial information with affiliates and joint marketing partners. However, such sharing prevents consumers from exercising control over the dissemination of their personal financial information. In addition, we believe that these entities already have access to the information needed, and that credit grantors and CRAs must use resources already at their disposal to prevent this crime. CRAs have the ability to monitor credit files for evidence of fraudulent activity, and should do so for all credit files, at no cost. Finally, credit grantors must heed fraud alerts consumers have already placed on their credit files, and request credit reports using at least four identifiers from the applicant.

Increasing Criminal Penalties is Insufficient

Despite passage of the Identity Theft and Assumption Deterrence Act of 1998, which made the theft of personal identifying information a crime, commissions of this crime continue to skyrocket. It is therefore more important that industry practices that allow thieves to exploit the system be addressed. In May 2003, CALPIRG Education Fund released the results of its interviews of with a sample of law enforcement officers from California and other cities with a high incidence of identity theft. Based upon the interviews, researchers concluded that: 1)

[3] The results of a limited survey conducted on the prevalence of problems with consumer credit reports appeared in the July 2000 issue of Consumer Reports. In the survey, Consumers Union staffers and others requested copies of their credit reports. One participant, a "Junior," found that his files contained information that belonged to his father, a "Senior." Others found that they were given the records of total strangers. Identity thieves benefit from this improper mixing of files, because imposter-generated fraudulent activity is easily mixed into the consumer report of an innocent victim.

identity theft is on the rise; 2) such crimes often remain unsolved; and 3) law enforcement officers believed that credit lenders should meet stricter requirements to ensure that credit is not granted to identity thieves. In fact, over 85% of officers responding believed that credit lenders must revise their practices.

Conclusions and Recommendations:

This hearing is entitled "Fighting Identity Theft -- The Role FCRA." In summary, we believe that current operation of the FCRA federal preemption, and allowable industry practices are, to a great extent, responsible for the skyrocketing number of cases of identity theft. Although thieves have become more sophisticated and organized, and the problem more widespread, the basic elements placing consumers at risk have not changed, and continue unabated.

We urge this Subcommittee to work to pass meaningful legislation that will address the elements of the FCRA and industry practices that help make commission of this crime possible. As stated above, we do not believe that the answer to the burgeoning crime of identity theft is to allow the financial services industry to have increased and unfettered access to consumer information. Instead, part of the solution lies in requiring industry to better manage and safeguard information already at their disposal.

We believe that the current preemption of state laws must be allowed to expire so that states can act quickly to address emerging methods of committing identity theft crimes. Thus far, states have been the most responsive and effective source of solutions to this growing problem. In addition, we believe that the consumer must be empowered with more control over the dissemination of their personal information to prevent identity theft, as well as with additional tools to clear their name if they do find that their good name is in jeopardy.

Changes to Industry Practice:

- Ban the commercial use of Social Security numbers.
- Increase penalties for furnishers that reinsert information in a consumer's credit file that had been previously disputed by consumer as inaccurate, and had been removed from the credit report by CRAs.
- Require CRAs to notify consumers at the original address when an address change is made to their report.
- Require companies to safeguard consumer financial information, and to notify them if the security of the information held is compromised.
- Require credit card number truncation.
- Require CRAs to alert consumers, free of charge, when suspicious activity is observed on the report (e.g. change of address, multiple inquiries, other indicators).
- Prohibit CRAs from releasing consumer information unless they have made a careful matching of a minimum of 4 identifiers (e.g. a unique identifier, full name, current address, previous address, and/or date of birth).
- Prohibit furnishers from selling debt to a debt collector where the consumer is an identity theft victim with respect to the debt in question.
- Extend the provision in the law with respect to the duty of "reinvestigation" to apply to furnishers. Currently the consumer must contact the CRA to dispute items on a credit report, and cannot initially seek correction of a disputed item from the furnisher itself.

Empowering Consumers to Prevent I.D. Theft and Clear Name:

- Allow consumers to easily monitor their credit files. Allow consumers to obtain, at no cost, a copy of their credit report and credit score from the three major CRAs.[4]
- Clarify that despite any ambiguity under the provision of FCRA, under the provisions of Graham-Leach-Bliley, states may pass stronger laws to give residents greater control over their personal information.
- Give consumers control over the sharing of personal information among companies, including affiliates.

[4] Six state currently allow consumers to obtain free credit report/s annually (Colorado, Georgia, Maryland, Massachusetts, New Jersey, Vermont). A few states cap the fee a CRA can charge.

- Improve consumer rights to enable victims of identity theft to more easily remove erroneous information from their credit reports.

- Create an easy system for consumers to place fraud alerts on their credit reports. Increase penalties on creditors that grant credit when there is a fraud alert on the account.

- Allow victims of identity theft to have access to creditor records (such as applications and transaction records) on accounts fraudulently opened in their name.

- Allow victims of identity theft to freeze their credit reports to prevent identity thieves from accessing any more credit in their names.

- Allow consumers to block accounts on their credit reports that appear as the result of the fraudulent activity of the identity thief.

- Victims currently are burdened by a nightmare of phone calls, and affidavit filings to clear their names. Create a central location and phone number as a resource for consumers to clear their names if they become a victim of identity theft.

Law Enforcement

- Increase the two-year statute of limitations for prosecution of criminals engaging in identity theft, and make the time run from the time of discovery of offense.

If implemented, we believe these measures could play a significant role in reducing the incidence and effects of this crime. I thank the Chairman, Ranking Member Sanders, and the Subcommittee for the opportunity to testify, and I look forward your questions.

Testimony of Amy Hanson
President
FACS Group, Inc.
Financial, Administrative Credit Services
(A Subsidiary of Federated Department Stores, Inc.)
Mason, Ohio

on behalf of the

National Retail Federation
before the

House Financial Services Committee
Subcommittee on Financial Institutions
and Consumer Credit
June 24, 2003

PREPARED STATEMENT OF AMY HANSON
PRESIDENT, FACS GROUP, INC.
Financial, Administrative Credit Services
(A Subsidiary of Federated Department Stores, Inc.)
MASON, OHIO
REPRESENTING THE NATIONAL RETAIL FEDERATION

Good afternoon. My name is Amy Hanson. I am President of the FACS Group, Inc. (Financial, Administrative, and Credit Services), which is a subsidiary of Federated Department Stores, Inc. I am testifying today on behalf of the National Retail Federation. I would like to thank Chairman Spencer Bachus and Ranking Member Mel Watt for providing me with the opportunity to testify before the Subcommittee on Financial Institutions and Consumer Credit about the growing problem of identity theft and the steps that FACS is taking to curb our losses and protect our customers from these crimes.

By way of background, The FACS Group is headquartered in Mason, Ohio and provides credit and other services to Federated Department Stores, Inc. Federated Department Stores is comprised of seven merchant nameplates: Macy*s, Bloomingdales, Burdine's, Rich's, Lazarus, Goldsmith's and The Bon Marche. We issue our proprietary credit cards under these names.

The National Retail Federation (NRF) is the world's largest retail trade association with membership that comprises all retail formats and channels of distribution including department, specialty, discount, catalogue, Internet and independent stores. NRF members represent an industry that encompasses more than 1.4 million U.S. retail establishments, employs more than 20 million people—about 1 in 5 American workers—and registered 2002 sales of $3.6 trillion.

In fiscal 2000, FACS reached a peak for identity theft related losses with 5,678 cases representing a total expense of $7.8 million. In the past two years, we have experienced a decline of approximately 33 percent in the number of identity theft cases and recognized a $3.2 million reduction in expense from ID theft. In the last six months we have seen a 41% improvement in ID theft cases compared to last year.

Mr. Chairman, instant credit represents about 93 percent of all new accounts opened at Federated Department Stores. As you know, this process is most likely to take place at the point of sale and relies on a highly automated and relatively quick procedure to verify an applicant's identity and check that individual's credit report. In order to cut down on fraud and identity theft during the instant credit application, FACS has implemented several procedures, systemic solutions, and other tools to identify potential ID theft victims. The primary focus of these initiatives is to detect discrepancies in the application information, check the application data against our known fraud information, and review the credit bureau report for a possible Consumer Alert or Fraud Alert reported by a consumer. If any of the above circumstances exist, extra verification is required. If any of the discrepancy information cannot be verified, we decline the application.

Our screening for fraudulent behavior does not stop after the application has been approved. All transactions purchased on our proprietary cards are reviewed through an algorithm, which includes logic to detect high-risk merchandise purchases, high dollar purchases, velocity checks, or payments on recently opened accounts. In addition, we systemically prevent the mailing of a credit card where a customer has recently changed an address.

One of the most important assets we use to stop identity theft is our known fraud information file. This known fraud file contains actual fraud information that has been reported from all Federated affiliated divisions. If an identify theft situation occurs in Bloomingdale's, our fraud investigation team will load this information into the known fraud file. Thus, if the perpetrator tries to apply at Macy*s, the information will match records in the known fraud file and stop the application process. By sharing the fraud information from Bloomingdale's to Macy*s (and other Federated Department Stores affiliates), we can successfully stop additional ID theft cases. The known fraud file is especially powerful because it is used to screen applications for credit, changes to accounts (address changes) and mail, phone, or internet orders. Last year, this known fraud file not only

stopped 674 cases of identify theft or account takeover, it also helped create a deterrent factor.

Currently, Federated Department Stores will take mail, phone, or internet orders. Regardless if the tender is made with our proprietary card, or another 3rd party card, we perform address verification on all orders. If a proprietary card is tendered on a FDS merchant web site like Macys.com, we verify the billing address provided to the Macys.com merchant with the actual address listed on the proprietary credit file (i.e. Rich's credit card). In addition, all address information is cross-referenced with our known fraud file discussed above. We also review high-risk merchandise (jewelry or gift cards), high dollar orders, and employ systemic edits to check for multiple orders being shipped to the same address. These controls proved very successful in 2002, reducing approximately 2,200 fraudulent disputes compared to 2001, which is a 65 percent reduction in fraud.

In addition, our Fraud Prevention group utilizes a vehicle to cross-reference UPC information on Internet orders to obtain descriptions of merchandise and an affiliate fulfillment system to search multiple orders across affiliate chains. This ability proved very helpful in discovering an Internet fraud ring where perpetrators were buying (with different credit cards and web-site affiliates) several orders of the same merchandise, then shipping these items to various addresses in the US. The perpetrators were then collecting the items for shipment overseas. We also found the fraud ring was using internet chat rooms to advertise a moneymaking opportunity that would obtain shipping addresses, and offering $50 per address to reship to Africa. This scheme was devised to usurp our address velocity counts mentioned above and purchased across our affiliate merchant sites to avoid detection. Fortunately, we were able to uncover and shut down this ring using our affiliate sharing tools.

It is important to note that we take the safeguarding of our customers' information very seriously. We also take pre-emptive measures to catch fraudulent transactions. We utilize neural network technology or rules-based systems to detect out of pattern shopping,

account changes, or suspect authorized buyer additions. Based on an unusual pattern or activity, we will make a call to the customer to confirm the questionable activity. Our customers view these calls as proactive steps to ensure the security of their credit. We also only release customer information over the phone with provision of security information to verify the identity of the customer.

We take these and other actions to protect our customers, because if we fail in that effort, our customers will view us in a negative light. This is the most important factor that drives our initiatives to stop fraud, and protect the customer. In the unfortunate event fraud does occur, we move just as aggressively to make the customer whole and restore their confidence. Our customers are never liable for any fraud transactions committed.

Some cases of our fraud include account takeover and check kiting (passing bad checks). We have been able to mitigate these losses by utilizing a cross-reference function when a bad check is received. This function searches for other accounts in other affiliated stores that may be exposed when an account takeover/check kiting situation exists, and then restrict the account from fraud activity.

Occasionally, we are able to definitively detect an attempted fraud and arrest the identity thief in our store. This usually occurs if our credit office, after being alerted during the application process, can quickly get in touch with the victim by calling a phone number that was provided through the credit bureau information. We will then ask if they want to pursue an arrest of the person attempting to use their personal information to open a credit account. If they agree, the store Loss Prevention department will detain the suspect and contact the police.

Mr. Chairman, I would like to be able to tell you that FACS has prevented 100 percent of all fraudulent credit applications this year, but I can't. The FACS Group, Inc. alone invests almost $1 million per year to identify, detect, and prevent fraud from being committed against our customers. This expense does not include the tens of millions

spent for in-store and corporate security at each of the Federated Department Stores' locations or headquarters.

The 33 percent reduction in ID fraud cases is a direct reflection of these preventative steps discussed above and focused attention to stop fraud. Unfortunately, identity thieves work just as hard to bypass our systems and were successful in 2002, at a rate of 7 per every 10,000 applications processed – less than one-seventh of one percent (0.07%). These cases of identify theft are not the result of flawed systems or procedures, but the strong determination of criminals to perpetuate fraud. Seeking out avenues to steal identities and commit identify theft is their full-time job. These individuals or rings have the ability to counterfeit, print, and laminate identity documents; even state issued ID cards or driver's licenses. These manufactured documents look and feel genuine.

Thieves always look for the path of least resistance, and then exploit it. Some will even publish web sites or use internet chat rooms to describe step-by-step processes to commit fraud. Today, identity theft and account takeover are the current trend for fraud. Both of these crimes rely on being able to present yourself using someone else's identity or personal information. Criminal rings with the technical equipment, know-how, and determination to obtain and abuse personal identities make stopping fraud an extremely difficult task.

For these types of criminals there is very little else we can do to detect and prevent the crime, and are looking to the states and the federal government to begin producing the most secure and foolproof identity documents possible. In addition, we look for opportunities to validate these identity documents real-time. Responsible sharing of information and providing the ability for retailers and other businesses to validate, at the time of presentment, a state issued ID or personal information yields the ability for instant authentication. The ultimate goal is uniform: to confirm the identity of the customer is not compromised at the time of a transaction. Other options include the use of biometrics or magnetic strip authentication to verify an individual's identity. Whatever the avenue of

choice, it is in the collective interest of retailers, banks and governmental bodies alike to make identity security a top priority. As you know, NRF is in the beginning stages of creating a public-private partnership to focus on identity security and its implications for both preventing identity theft as well as helping victims put their credit records back together again.

It is also critical that we pursue tougher law enforcement statutes on identify theft criminals, especially multiple offenders. The current environment pits thieves against businesses, but uses stolen consumer personal information as the means for the reward. This situation demands an effective deterrent against committing identity theft.

As stated above, identity theft represents such a small piece of total credit applications. Identity thieves bank on this statistic and the difficult task to match the personal name of customers to the real person. This is especially difficult in the current age of technology that allow others reproduction or creation of counterfeit documents virtually anywhere. The task at hand is for retailers to "know" the customer, and the demand from customers is to accomplish this without being inconvenienced. The only way to accomplish this goal is through the use of information.

As you know, Identity theft is a crime with at least two victims, the individual whose identity was stolen and the businesses that bear the financial cost of the crime. Clearly, it is the individual victim that is most directly hurt, but, if identity theft crimes continue to rise at the rate reported by the FTC, all consumers will ultimately pay as business losses are passed back to customers. Also, if a customer is victimized by fraud, and the fraud occurs in a Federated store, that customer is going to have a negative impression of our name and our ability to prevent fraud. We need our customers, and their confidence. However, we also know that perpetrators probe our systems daily for opportunities to commit fraud. The ability to react to new trends is paramount for us to protect our consumers. As such, it is critical that our access to information and prevention opportunities continue. The identity theft criminals adapt and change quickly, we need that same flexibility.

In closing, I would like to emphasize the retail industry's strong support for the permanent reauthorization of the seven areas of preemption contained in section 624 of the Fair Credit Reporting Act. The current uniform national standards allow retailers and lending institutions to get a complete and accurate picture of a person's credit history as well as prevent fraud and identity theft. Consumers have come to expect efficient and secure access to credit when purchasing everything from an automobile to consumer goods such as furniture, appliances and apparel. In the final analysis, we in the retail industry have a real concern that a more fragmented approval process for credit would actually negatively impact consumers, and increase their exposure to identity theft. In addition, curtailing the flow of information would clearly negatively impact retail sales, ultimately costing jobs and hurting the economy as a whole.

I appreciate the opportunity to testify here today. I look forward to answering your questions as well as those of the Committee. Thank you.

TESTIMONY OF

JAMES K. KALLSTROM
SENIOR EXECUTIVE VICE PRESIDENT
MBNA AMERICA BANK, N.A.

BEFORE THE

FINANCIAL INSTITUTIONS SUBCOMMITTEE
COMMITTEE ON FINANCIAL SERVICES
UNITED STATES HOUSE OF REPRESENTATIVES

HEARING ON

FIGHTING IDENTITY THEFT

2128 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, D.C.
JUNE 24, 2003

INTRODUCTION

Thank you Mr. Chairman for inviting me here today. I think I can safely speak for the entire industry in complimenting the committee for the thoroughness with which you are examining the issues relating to reauthorizing the Fair Credit Reporting Act. From our perspective, you have constructed a compelling record from which to legislate and we have high praise for the diligence and dedication of the staff who have brought all of this together.

Regarding identity theft, we are in complete agreement with you and the other members. Identity theft – like other serious crimes - is an attack on our citizens, our businesses, and on our economy. It accounts for only about four percent of the fraud we experience but, as you have just heard, it often exacts a personal cost of time, reputation and frustration that is very hard to measure.

I have years of experience dealing with the crime of identity theft and, unquestionably, more, much more, can and should be done in each of four aspects - - prevention, detection, enforcement and victim assistance.

The issues relating to identity theft are very often quite complex. They run the gamut from the common phenomenon of theft by a family member, friend or associate to how we can more quickly restore the good name and credit reputations of unwitting victims. Viable solutions likely will involve greater participation by all of us - - the credit granting industry, retailers, the credit bureaus, law enforcement, prosecutors, government agencies, and consumers.

No one disputes that identity theft is a serious crime that should be attacked vigorously. It also is a crime that victimizes consumers and industry alike. And as with many crimes, the cliché "forewarned is forearmed" applies. Insuring the availability of and arming both businesses and potential victims alike with key information goes a long way toward prevention and apprehension. As Assistant Secretary Abernathy remarked recently, "Identity theft is not caused by information. It is caused by a *lack* of information."

SUMMARY

In summarizing my statement for the record, I would like to make four points.

First, the interests of our customers and the interests of industry are synonymous here. Our business philosophy is "find the right customers and keep them." We want our customers to be able to use our products – and use them securely. We want our customers to have confidence that we will help protect them against the scourge of identity theft.

When fraud does occur, our customers are not responsible for the fraudulent charges and we provide assistance both to help stop further damage and to help in recovering from the identity theft. But, as we have just heard, it is far more difficult to restore the confidence of victims and to relieve the effects of having their identities stolen. We agree with our customers who say, reputations, goodwill, financial well being and consumer confidence are all put at risk because of identity theft. In the end, it hurts everyone.

Second, prevention and detection of identity theft is what we do with every application and every transaction seven days a week, 365 days a year. We invest millions of dollars preventing and detecting identity theft and other types of fraud. We employ hundreds of people who specialize in fraud detection and prevention and have a sizable cadre of people dedicated to ensuring our customers are properly identified. We employ extremely sophisticated neural-networks and experience-based automated strategies to find and reduce fraud and identity theft. From exploring discrepancies between applications and credit reports to scrutinizing hundreds of thousands of daily transactions for anomalies, we fight identity theft from the credit application stage through loan repayment.

Our customers are critical participants in the process but there is no question that the Fair Credit Reporting Act is the foundation of this effort. To be successful, we rely upon the kind of uniform, current credit information that the FCRA has given us.

The third point I would like to make is setting the record straight on a couple things: affiliate sharing and prescreening. With affiliate sharing we are aware of no instance - not one - where affiliate sharing resulted in identity theft. To the contrary, it helps the industry fight identity theft.

Our experience with prescreening is similar: prescreening results in substantially fewer fraud attempts – not more. A study released last week by the Information Policy Institute (IPI), a copy of which I am submitting with my statement for the record, confirms that the same holds true for the entire industry. In fact, the study found that the industry losses from fraudulent prescreened applications amount to four one thousandths of one percent of total sales volume and eliminating prescreening would likely result in an increase in identity theft. That is so because prescreened offers reflect only names and addresses, less than is in a telephone book, and the prescreening process involves more filtering not less.

One final point: Assistant Secretary of the Treasury Wayne Abernathy understands the industry, understands the problem, and he and others at Treasury have talked about the need for a comprehensive approach to address the problem of identity theft. We agree that any approach should include enhanced prevention, detection and victim assistance. It should include reauthorizing FCRA because, as Assistant Secretary Abernathy says, to do otherwise risks "creating shadows," where identity theft can occur. On the enforcement side, the solution should include stiffer penalties reflecting the serious and pervasive nature of this crime.

We also agree that any solution should help consumers make more informed decisions about information sharing. This can happen by making privacy notices shorter, simpler and in plain English and making opt out procedures easier and uniform so that consumers can more easily exercise control of personal information and in a more meaningful way.

Everyone agrees that it would be of enormous benefit to provide consumers with easily digestible privacy notices that include easy opt out procedures. In fact, in a recent survey we found that our customers overwhelmingly support a simple, food label-like notice as the kind of notice they want – a notice they will actually read, that is easily comprehensible, and which allows busy people an opportunity to participate in information sharing decisions in a more meaningful way. It is simply a good idea that will be of great benefit to consumers.

In the end, legislating more and better tools for law enforcement, consumers and the industry to use to prevent, detect and recover from identity theft is a consumer issue that will help us all. We applaud your attention to these critical issues and I look forward to your questions.

HOW MBNA PREVENTS & DETECTS IDENTITY THEFT

MBNA proactively contains fraud by reviewing new applications for discrepancies when compared to credit reports and other available data, and by continuously evaluating Customer-initiated sales transactions and requests for credit. These controls can be grouped into three categories: the prevention of new account fraud, the prevention of fraud on existing accounts, and the detection of fraud on existing accounts.

A. New Account Fraud Prevention

In today's national credit market, all credit issuers are more vulnerable to fraudulent requests for credit due to the non face-to-face nature of the process. As in all key decision-making functions, MBNA emphasizes human judgment.

Identity verification begins immediately after a new application is received and entered into the system. The system compares data provided on the credit application to data returned from a credit-reporting agency but a real person reviews this information. In addition to credit report data, other tools used to assist hundreds of analysts in identifying discrepancies and suspicious activity include:

- experience-based strategies that identify potential anomalies
- a fraud scoring model
- consumer statements
- security alerts, and
- an internal fraud database

Moreover, our fraud analysts apply their experience and judgment to identify suspicious applications.

If the application is judged suspicious, analysts have available a variety of tools to verify information and, in many cases, are able to locate the actual applicant to verify the validity of the application by speaking with this person on the telephone. If fraud is identified, victims are instructed to contact each credit reporting agency to place a statement on their credit file to let other credit grantors know that they have been victimized. Additionally, victims are given a toll-free number to the Federal Trade

Commission (FTC) to obtain information about identity theft and to add their name to the FTC fraud database.

In addition, credit card issuers are required to report confirmed identity theft to an external fraud database known as Issuers Clearinghouse Service ("ICS"). ICS is jointly owned by MasterCard and Visa. The service provides notifications to credit card grantors about fraudulent or potentially fraudulent activity involving consumers' personal information. As a secondary precaution, we use ICS to review and compare new accounts to the ICS database to ensure that any suspicious activity is identified and investigated.

B. Existing Account Fraud Prevention - Authorizations

MBNA employs state-of-the-art authorization systems to prevent fraud. A variety of sophisticated statistical techniques allow the vast majority of our Customers to use their cards without interruption, while also identifying transactions that present a high degree of fraud risk. Since 2001, MBNA has received seven awards from MasterCard and Visa for the performance of this authorization system.

Empirically derived strategies are developed based on historical portfolio performance. Central to the strategies is the use of a customized fraud score that employs neural network modeling techniques to make decisions and learn from changing patterns of fraudulent activity.

Use of this technology has allowed MBNA to maintain industry-leading authorization approval rates. However, in order to mitigate fraud risk we still decline or ask a merchant to contact us on over 2 million transactions annually. Merchants who call in response to a referral request are routed to an analyst who validates that the person presenting the card is our Customer. Referral calls are always answered immediately and are handled 24 hours a day, seven days a week.

C. Existing Account Fraud Detection

Authorization strategies alone cannot contain fraudulent activity. MBNA employs hundreds of fraud analysts who evaluate unusual spending patterns and contact Customers to determine if they believe fraud is occurring on their account. The same statistical techniques and tools used to establish authorization strategies are used to develop and employ fraud detection strategies.

For example, MBNA requires all Customers to contact us to activate new cards. A similar approach is taken when requests for change of address or requests for access devices (cards, check, ACH, etc.) are made. At this stage, specialized MBNA people apply strategies specifically designed to prevent and detect unauthorized access to a Customer's account.

When a fraud claim is received, MBNA conducts investigation. When the fraud claim is accepted, the Customer is absolved of any financial responsibility resulting from the fraud and their credit bureau report is appropriately corrected. A fraud specialist will work with the Customer to discuss the appropriate steps that should be taken to protect themselves against future crimes and an identity theft brochure, which we created, is mailed that explains the process.

We will continue to investigate cases by filing a Suspicious Activity Report ("SAR") on appropriate accounts in accordance with Bank Secrecy Act guidelines. Moreover, we employ fraud investigators, former law enforcement officers that work with federal, state and local law enforcement agencies on identifying and prosecuting fraud perpetrators.

An important factor in minimizing fraud losses is the ability to review transactions quickly and thoroughly. Continuous investments in the fraud detection systems have created greater efficiencies and better methods for isolating the riskiest transactions and accounts. Isolating and prioritizing the fraud more efficiently lets us find the fraud sooner. Finding the fraud sooner contains the loss. For example, the following is an excerpt from a letter received from a Customer who recently experienced identity theft:

> *" We had a stranger trying to move our account to X in the quest to use our credit. You were able to catch this attempted identity theft early and inform us of all the proper avenues to pursue to keep our financial information safe. We applaud you. Your company consistently calls us with any suspicious activity or charge, which is very reassuring."*

Recent improvements have allowed MBNA to reduce the average balance for a fraud claim to less than 2001 levels. As a result, MBNA has been able to reduce fraud losses even with a growing loan portfolio.

HELP IS NEEDED TO COMBAT IDENTITY THEFT

We have a number of specific suggestions but in general, our experience convinces us that six categories need to be enhanced. They are:

- Greater national uniformity, not only with FCRA, but in most aspects of combating identity theft - lack of uniformity directly benefits identity thieves.
- Increased penalties, and increased resources for law enforcement training, investigation and prosecution of identity theft – the duties of law enforcement at all levels have grown tremendously in recent years – if we are serious about combating this particular crime, training and resources must be dedicated to it.
- Greater consumer participation through increased access and simplifying the notice and choice process – make information accessible, comprehensible, and make consumer choice informed and easy.

- Consistent with what Assistant Secretary Abernathy said last week, greater information sharing within the industry, especially along the lines of what The Consumer Data Industry Association (CDIA) recently announced about sharing of fraud alerts between the credit bureaus, and;
- Greater victim assistance once the crime has been established.

Specifically, we offer the following suggestions as well:

Training and Resources for State and Local law enforcement

Most identity theft investigations fall to local authorities. We applaud what Secret Service is doing to provide state-of-the-art training and think more should be done. Local law enforcement at the "first responders" need more training and resources given the rate of growth of this crime.

Standardized Reporting/Common Definitions

Because identity theft investigations are frequently multi-jurisdictional, a lack of common definitions and standardized reporting, particularly at the local level, is a significant problem that often results in cases not being investigated.

Increased Penalties

Many identity theft instances are not investigated because, even if proven, prosecutors will not expend scarce resources to prosecute because of the minor nature of the crime. Increasing the penalties substantially likely would raise both the number of prosecutions and the deterrence value.

Credit Card Number Truncation

The recent policy change to mandating truncation on all electronically printed receipts to include expiration date is strongly supported across the industry.

Nationwide Service of Process

The Patriot Act contains authorization for nationwide service of process when certain computer related electronic evidence is being sought. This was done because of the interstate nature of most investigations seeking electronic evidence. The same is true for identity theft. Frequently the victim and perpetrator are in different jurisdictions.

Centralized Data Base

Currently there is no central database accessible to both law enforcement and industry reflecting known fraudulent names, addresses, account numbers, etc.

Law Enforcement Coordinating Council

S. 1742 in the 107th Congress contained provisions to have a coordinating body for law enforcement on this issue. The more commonality there is between jurisdictions, the more it helps the industry deal with what is often a multi-jurisdiction issue.

Civil Restitution/Civil Forfeiture

Although the amounts may be small, forfeiture provisions that inure to the financial benefit of local law enforcement and create liability to the victims for actual damages could increase the cost to identity thieves and help victims recover what they have to pay out-of-pocket.

CONCLUSION

We agree with the approach taken by Assistant Secretary of the Treasury Abernathy - to be of maximum effectiveness, any approach to reducing identity theft should be comprehensive to better serve consumers, the government, the private sector, and, ultimately, the national economy.

The reauthorization of the seven preemptions added to FCRA in 1996 is a necessary starting point. As Assistant Secretary Abernathy says, to do otherwise risks creating shadows where identity theft can flourish. This is so because the FCRA, as amended, has provided a nationwide financial infrastructure that enables businesses to obtain immediate and reliable credit information on which to base key financial decisions but also to use in properly identifying customers and ferreting out identity thieves. And we should not forget, it has provided a mechanism that consumers rely upon every minute of every day to better their lives, and to aid in protecting themselves.

Finally, while we are investing millions in fraud detection and prevention strategies, and in people to assist our customers and maintain their confidence, we agree that more must be done across the industry, across the government and even by consumers if, collectively, we are to be successful.

Before the United States House of Representatives

Committee on Financial Services

Subcommittee on Financial Institutions and Consumer Credit

Testimony of Lee Lundy
Vice President, Consumer Services
Experian

www.experian.com

Lee Lundy
Experian
701 Experian Parkway
Allen, TX 75013

Introduction

For more than 50 years Experian has been a leader in the information industry. In fact, the company's roots date back more than 100 years to the pioneers of credit reporting. Its success is based on sound information values that guide the development of practices and policies that protect consumer privacy, ensure security and provide benefit to consumers and our business clients alike.

Responsible information use today affords consumers greater choice, convenience, and lower prices than ever before. In past decades, our economy was local. Businesses were located where consumers lived. Product and service choices were limited to what was available in a consumer's neighborhood, the local main street, or perhaps a nearby city. Consumers learned about businesses by walking down the street, or reading ads in the local newspaper.

Today we have a national credit reporting system. Businesses in Los Angeles and New York compete daily to sell financial products and services to consumers in Kansas. Where once there was only a single provider of a product or service, or maybe two or three to choose from, there now are hundreds. Because of responsible information sharing, those businesses can reach consumers who are most likely to need their products and services. That greatly increases consumer choice and promotes competition, which drives down prices.[1]

Today, consumers expect instant access to credit, affordable, high quality goods and convenient customer service 24-hours a day, seven days a week. Businesses in our "always-open" economy struggle to meet their customers' expectations of value,

affordability and convenience while at the same time protecting consumers and themselves from fraud and identity theft.

Every day Experian is on the front lines of the war against fraud because of its role as a leading information solutions provider, and because of its role as a consumer reporting agency. We are driven to provide the best fraud tools available so businesses can prevent victimization from occurring, and we strive to help consumers recover from fraud and identity theft as quickly as possible.

Economic crime cost U.S. businesses more than $1 trillion dollars in the year 2000.[2] According to a study by Meridien (July 2002), institutions absorb approximately $18,000 per identity theft including loss of goods, revenue and costs associated with customer service and victim assistance.

More than 1 million consumers contact Experian's National Consumer Assistance Center each month to request a credit report, get help with questions about their reports, or for fraud assistance. Every interaction is important, but none more so than helping consumers victimized by fraud or identity theft.

Experian worked with the U.S. General Accounting Office during 2001-2002 in researching fraud and identity theft. We found that approximately 30,000 consumers add fraud victim statements to their credit histories each year.[3] The number includes individuals who are not victims, but who are concerned about fraud and identity theft,

---

[1] Fair Credit Reporting Act: Access, Efficiency & Opportunity; the Economic Importance of Fair Credit Reauthorization. Information Policy Institute; June 2003
[2] From studies by the American Bankers Association (ABA), BAI, Cellular Telephone and Internet Association (CTIA), Coalition Against Insurance Fraud (CAIF) and UN.
[3] Identity Theft: Prevalence and Cost Appear to be Growing, GAO-02-363, March 2002

and not all victims add a statement to their credit history. Therefore, this figure does not represent a precise number of victims.

Clearly, fraud and identity theft are serious crimes that affect consumers and businesses across all industries, among them financial services, health care, insurance, cellular services, utilities, retail, technology and online commerce.

Our experience in business fraud prevention has shown us what works and what does not work in the battle against fraud and identity theft. When fraud does occur, we are in the forefront of consumer fraud victim assistance.

What works in the fight against fraud

The most effective strategy in the war against fraud is responsibly using the free flow of information to enable cooperation among the national credit reporting agencies, businesses, law enforcement agencies and consumers to effectively prevent and fight the crime. Fraud and identity theft can be curtailed only if we all work together effectively and efficiently.

Helping businesses stop fraud

Businesses must work together, as well as with Experian and other information service providers, to identify fraudulent activity and prevent proliferation of the crime at the point of application.

Today, there are highly effective tools to fight fraud and identity theft. Information services providers are in a position to help develop and implement those tools because of the data they collect, maintain and manage. Experian has invested heavily in developing the industry's leading fraud prevention and detection tools. Our

expertise with traditional data sources and ability to develop new tools based on responsible information sharing have enabled us to create some of the industry's most effective fraud detection and prevention systems. Our goal is to help businesses prevent fraud at its origin. Targeting prevention reduces business' fraud losses, protects consumers from fraud and eliminates the challenges of victim assistance.

Among the most effective ways to fight fraud and identity theft is by sharing information about known fraudulent activity as part of a cooperative database, such as Experian's National Fraud Database. The National Fraud Database is comprised of known, verified fraudulent activity provided by businesses from across industries. The database alerts users to information associated with verified fraudulent activity enabling them to stop fraud before it starts.

Experian's Detect service, another cooperative database, takes fraud prevention to the next level by comparing application information for anomalies that may indicate fraud.

The online environment poses its own unique set of challenges to fraud prevention. The most difficult issue is authenticating the identity of a customer whom a business will never meet face-to-face. Our Authentication Solutions are designed to prevent online fraud by requiring customers to pass an "identity quiz" which includes questions from a number of sources. Customers are asked questions to which only they are likely to have the answers. The questions are drawn from credit history information and other sources. The various data sources are essential because they enable businesses to ask questions that have answers that would not be found in a stolen wallet, which

commonly includes identification elements such as name, address or even Social Security number.

With the National Fraud Database, Detect and Experian's Authentication Solutions, lenders are equipped with some of the most effective fraud and identity theft prevention tools available today. *(Appendix A: Experian's Business Fraud Services, p. 18)*

For example, one national credit card issuer realized a 13 percent decrease in application fraud losses and annual savings of $18 million by implementing only one of Experian's most basic identity authentication tools. Businesses utilizing Experian's fraud prevention tools often report decreases in fraud losses of 50 percent or more within the first year of implementation. Similarly, a national telecommunications provider experienced a 55 percent decrease in fraud losses per handset and decreased the time it took to confirm fraud records by more than two-thirds. *(Appendix B: Experian cases studies, p. 21)*

The consumer's role

Consumers, too, play an important part in protecting themselves from identity theft. Much of what they can do is simple. Experian, through its consumer education materials, consumer advocates and government agencies recommend that consumers:

- Sign their credit cards as soon as they receive them.
- Store credit cards and other identification documents in a safe place.
- Do not carry identifying information in a purse or wallet that the consumer does not need, such as a Social Security card.

- Do not carry in a purse or wallet more credit cards than necessary. For instance, carry only the one or two cards the consumer uses most.
- Do not provide sensitive information over the telephone unless the consumer initiated the call, trusts the business or individual with which they are speaking and understands why the information is needed.
- Do not write driver's license or Social Security numbers on postcards or the outside of envelopes.
- Do not leave receipts at the sales counter, ATM machine or fuel pump.
- Shred all documents containing sensitive identifying or financial information before discarding them.

Online shopping offers great convenience and opportunity, but similar common sense actions apply:

- Do not provide sensitive identifying or financial information in response to an e-mail message unless the consumer initiated the communication.
- Conduct transactions only through secure connections.
- Only shop online with reputable, known businesses with posted privacy policies and clear merchandise satisfaction and return policies.
- Subscribe to a monitoring service that alerts the consumers when their credit history has been accessed.

The importance of law enforcement

While sophisticated fraud prevention tools and effective victim assistance are critical, strict enforcement of anti-fraud laws is equally important. Experian and our credit reporting counterparts worked with the Federal Trade Commission to establish a uniform fraud affidavit to make reporting fraud easier. We block any account reported as fraudulent when a valid police report is provided by the consumer, effectively suppressing the fraudulent information immediately from the credit history. Yet, it remains difficult for consumers in many instances to obtain a police report because of jurisdictional issues.

Conversely, credit repair clinics and others who hope to alter or delete accurate, negative information from consumer reports have falsified police reports provided to Experian and the other consumer reporting agencies.

Improved multi-jurisdictional law enforcement efforts are essential to solving the fraud problem. Consumers often find themselves being sent from precinct to precinct and agency to agency. Some agencies are unwilling or unable to issue a report, and all of them lack sufficient resources to conduct a thorough investigation. Resolving jurisdictional conflicts and sufficiently funding enforcement are essential actions for winning the battle against fraud.

Until recently, law enforcement kept few meaningful statistics on fraud and identity theft. Such statistics are important to better understanding the extent of identity fraud in its various forms. There are many types of fraud including account takeover, "friendly" fraud in which the victim knows or has a relationship with the perpetrator, and

true name fraud. Some statistics suggest that up to 40 percent of all identity fraud is perpetrated by a family member or by someone the victim knows.

Better defining the prevalence of the various fraud types and the ways in which they are perpetrated will enable more effective law enforcement and development of meaningful protective measures by the private sector.

Improved relationships between victims and law enforcement agencies are also important. Too often, consumers are not seen as victims by law enforcement. Rather, businesses are viewed as the victim because they usually suffer greater monetary loss. Maintaining a closer relationship with consumers, assuring them that an investigation is taking place, notifying them of progress, and updating them on prosecution are important steps in victim assistance.

Stronger penalties against those who perpetrate financial fraud are needed. Current penalties are inconsistent and range from probation to imprisonment. Penalties must have teeth to be effective, and they need to be consistent from jurisdiction to jurisdiction.

Consumer victim assistance

Unfortunately, identity theft has already occurred by the time a fraudulent account becomes part of a credit report. In some cases, a full understanding of the breadth of the crime may not be known for some time. Identity theft, unlike other crimes of theft, often occurs over a period of weeks or perhaps months. It is frequently a longitudinal crime – different than a burglary. Therefore, when you hear reports in the media that it took a consumer months to unravel financial records affected by identity theft, it is often the case that elements of the criminal activity did not reveal themselves until weeks or

months later. When a victim identifies a fraudulent entry on a consumer report, we work promptly with the provider of the information and the consumer to resolve the issue. At that point, our role as a consumer reporting agency becomes one of victim assistance.

Experian and our counterparts work together continuously to develop victim assistance processes that are as uniform and efficient as possible. In 2000 we launched, in conjunction with the Consumer Data Industry Association (CDIA), a series of voluntary initiatives designed to improve consumer fraud assistance. These include standardized, industry accepted, computer-readable security alerts and, victim-assistance best practices. Among the identified best practices are notices to creditors, automated systems enabling 24-hour, seven-day-a-week addition of fraud security alerts, and free credit report monitoring. *(Appendix C: CDIA Consumer Fraud Victim Assistance Initiatives, p. 23)*

Most recently, we announced a one-call fraud alert program. Today, victims need only contact one credit reporting agency to have a security alert added to all three credit histories. Consumers no longer need to call each of the three national credit reporting agencies to add fraud alerts, have a complimentary report mailed and activate the CDIA fraud initiatives. By simply notifying one of the agencies they will begin the fraud recovery process at all three, making the recovery process easier and faster.

Consumer reporting agencies are all committed to ongoing improvement of our victim assistance services *(Appendix D: Experian's Consumer Fraud Victim Assistance Process, p. 25)*, but the battle against fraud and identity theft can only be won by preventing the crime at its source.

What does not work in the fight against fraud

Our experience has also shown that many approaches perceived to increase fraud prevention and aid recovery actually result in neither. Those approaches include restricting data flows and providing free credit reports. At face value, both seem to promise greater fraud protection. In reality, they do little to protect consumers and in fact may make the fraud problem worse.

Restricting data flows

Access to and responsible use of information from a broad spectrum of sources is essential to our fight against fraud and identity theft. The success of sophisticated fraud detection and prevention tools depends on continued access to key identifying information and responsible information sharing.

This is especially true when considering the growing numbers of application fraud and transactional fraud, which occur most often when a credit card cannot be presented to the business, for example in tele-commerce and Internet transactions.

Solutions to these types of fraud demand tools that can utilize complete, accurate and current information from multiple sources. Eroding the ability of businesses to obtain and share information responsibly and to compare that information with consumer-supplied information will increase the risk of fraud and identity theft, reduce competition and drive up prices.[4]

[4] Fair Credit Reporting Act: Access, Efficiency & Opportunity; the Economic Importance of Fair Credit Reauthorization. Information Policy Institute; June 2003

Closing public records or limiting the information in them, deleting, truncating or redacting Social Security numbers, limiting or eliminating business-to-business uses of Social Security numbers and other information restrictions exacerbate the fraud problem.

Experian and other responsible fraud solution providers are dependent on public records as a source of accurate identifying information essential to victim assistance and fraud prevention services. Legislative restrictions on the use of information do little to deter serious identity thieves. They will simply obtain the information through other means, illegally if necessary. The effectiveness of victim assistance and fraud prevention tools, however, is seriously degraded because critical data elements are lost.

Social Security numbers (SSNs) often are described as the key to committing fraud. As a result of that characterization, deletion or redaction of SSNs from public records and closure of public records that include SSNs is threatening the availability of public records for fraud prevention. While it may seem counterintuitive, such actions actually result in greater exposure to fraud.

An alarming example now before Congress is a proposal sponsored by the U.S. Judicial Conference that would truncate SSNs in bankruptcy records, even when provided to consumer reporting agencies. Congress should reject or modify the proposal or the accuracy and completeness of bankruptcy information contained in consumer reports will be diminished.

Truncation of SSNs is as damaging to fraud prevention as complete deletion or redaction. The ability to match only a portion of an SSN is not sufficient for fraud detection or prevention. Variations or anomalies in the unseen portion of the number could indicate fraud that would go undetected. Equally important, truncated account

numbers are not adequate for differentiating between individuals, particularly if they share a common name, such as John Smith or Jim Johnson, for example, or a close relationship, such as twins, whose SSNs may vary by only a single digit. Also consider that 4.5 million consumers have one of two surnames (Smith or Johnson) and that 3 million people change their last name each year and SSN truncation becomes a very significant impediment to successful fraud detection and prevention. The result of truncation is the same as complete deletion of the number: increased fraud risk, not increased protection. Therefore, Experian respectfully requests that Congress review and comment on the U.S. Judicial Conference proposal.

Free Credit reports

Free credit reports also have been touted as a solution to the fraud problem. A free credit report actually has little impact on fraud prevention. As mentioned previously, by the time fraudulent accounts appear on a credit history the crime has already been committed.

Current FCRA provisions already provide free reports for virtually all consumers who need a credit report. For instance, federal law already requires credit reporting agencies to provide a free report to consumers whenever an adverse action is taken, whenever a consumer believes he or she may be a victim of fraud, and in situations where the consumer is either unemployed or receiving welfare assistance.

Credit reporting agencies also are mandated to provide toll-free consumer assistance after providing a free report. Costs of mailing a report and maintaining a call center, including staff and infrastructure such as telephone service, must be evaluated when considering the true cost of a "free" credit report. Furthermore, the $9 fee allowed

by the FCRA enables credit reporting agencies to recoup only a portion of the expense associated with providing the report and subsequent consumer assistance.

Those who promote free reports do so in order to enable consumer "access" to their reports, but this is a "red herring." Consumer reporting agencies readily grant access 24-hours-a-day, 7-days-a-week, every day of the year. There is no evidence that the $9 fee applicable when a free report is not otherwise mandated is a barrier to access.

Today, a serious but often overlooked factor associated with proposals to extend free reports to all without condition are the costs involved with providing trained consumer assistance professionals who can answer consumers' questions. While the cost of the actual report is one expense, staffing to meet this exposure is something we do not have the physical space or financial capacity to undertake.

Another challenge to us is meeting the exposure created by businesses and government agencies outside the credit allocation stream that direct hundreds of thousands of consumers to obtain a free report under the claim of fraud, when in fact no fraud or identity theft occurs. For example, in a recent case during just a few days, the credit reporting agencies were inundated with thousands of requests for free reports when computer equipment containing information about more than 500,000 consumers was stolen from Tri-West, a Department of Defense subcontractor in Arizona. Yet, not a single instance of fraud or identity theft associated with the theft has been reported.

Likewise, the concept of notifying consumers of computer security breaches will do little to protect them from fraud, but will likely result in unnecessary concern and fear.

Literally thousands of attempts to hack into computer systems are made across the country every day. Sophisticated firewall and security systems thwart virtually all of

those attempts. When an attempt does succeed, it does not always result in the information accessed being used for fraud purposes. Last year, for example, nearly 200,000 consumers were directed to ask for a free report when a State of California database of employee records was compromised.

Just as in the Tri-West case, there has been no evidence that fraud or identity theft has been committed. However, all of the employees were instructed to get a free report under the claim of fraud.

Still, under current notice proposals virtually every successful hacking incident would result in notices and free reports being sent to hundreds-of-thousands of consumers who are unlikely to become victims of identity theft.

Such instances impose tremendous costs on credit reporting agencies and harm consumers who have urgent needs by flooding our consumer assistance centers -- at our expense, not at the cost of Tri-West, the State of California or other businesses responsible for security breaches. Adding a requirement to provide free reports and the associated consumer assistance responsibilities to 200 million consumers would simply be unmanageable in terms of our ability to control costs and meet currently required service levels.

Conclusion

As identity thieves become more "creative" in their attempts to commit fraud, the ability of organizations fighting fraud to access and utilize information from a range of sources becomes increasingly important.

We are allies in the war against fraud. Our enemy is the same. Unfortunately, currently popular legislative and regulatory proposals -- the legal bombs in the battle --

are being dropped on the wrong targets. By eliminating the ability of information solutions providers, like Experian, to access and utilize data from a broad range of sources, you inadvertently destroy the most powerful arsenal we have against fraud.

The key to Experian's fraud services, all fraud prevention tools for that matter, is responsible information use. The most effective fraud tools rely on many data sources to ensure accurate identification. Access to that data, and the ability to utilize it responsibly must be protected.

Appendix A: Experian's Business Fraud Services

Experian has long provided tools to identify increased fraud risk and has during the past several years introduced a number of groundbreaking services to help businesses prevent fraud and reduce fraud losses. The most powerful weapon against fraud is responsible data use.

Users of credit reports have long had the following services available:

Consumer fraud alerts: For many years, consumers have been able to add to their credit histories security alerts, indicating they may be a fraud or identity theft victim and victim statements stating that they are victims. A security alert on an Experian credit history remains for 90 days and warns lenders that the consumer may be a victim, enabling the lender to take additional precautions. The temporary security alert is added automatically when a consumer selects the fraud option on Experian's automated telephone system or Internet site. A credit report will be provided automatically, either by mail or online, which will include contact information to speak with a trained fraud representative. Consumers who know or believe they are fraud victims can request that a 7-year victim statement be added to their credit history after receiving their credit report. A victim statement indicates the consumer is a victim and asks that the lender contact them at a telephone number provided by the consumer before granting credit in their name.

FACs+: An automated system that identifies information in a credit history that indicates increased fraud risk. Indicators include addresses recorded as belonging to a business, Social Security numbers reported as belonging to a deceased individual, Social Security numbers that have not been issued, or variations in names or addresses, among

others. The FACs+ statements do not indicate fraud is occurring, but rather that information in the credit history suggests higher fraud risk.

Fraud Shield[SM]: A fraud prevention tool that goes beyond the simple single-element identifiers of FACs+ and compares data throughout the credit history to more accurately define fraud indicators. Like FACs+, Fraud Shield[SM] does not indicate fraud is or has occurred, but instead indicates to lenders that information suggests a higher fraud risk. Fraud Shield[SM] enables lenders to take additional precautions to protect consumers and themselves from fraud when considering applications.

More recently, Experian launched new fraud detection and prevention tools that utilize data beyond that in a credit report and that aid businesses in both online and offline environments.

Authentication Services: Experian's Authentication Services protect business and consumers from fraud and identity theft in the online environment. Authentication Services not only review common "in-wallet" identifying information such as name, address, date of birth and Social Security number and driver's license number. The system also requires "out of wallet" information that only the consumer would know, such as what lender holds a mortgage, balances (in a range) on credit cards, or what type of car an individual owns. Data is drawn from a variety of sources including credit histories and property records.

National Fraud Database[SM]: Experian stepped to the forefront of fraud and identity theft detection and prevention with the introduction of the National Fraud Database[SM]. It is the first industry-wide database of known and verified records of

fraudulent activities identified by National Fraud Database subscribers and consumer fraud victims.

National Fraud Database reports are used during the application process for credit or banking services, account reviews and other activities allowed under the FCRA. The information in a report helps lenders identify not only when fraud is potentially occurring, but also when they are working with a victim, enabling them to take appropriate actions for each circumstance.

Detect[SM]: A further advance in fraud detection and prevention, Detect[SM] provides on an online system that notifies credit grantors of potentially fraudulent or high-risk applications that would likely have been accepted through normal automated underwriting procedures. The system relies on incoming application information, past application data and credit bureau information to trigger fraud warnings. Detect[SM] identifies inconsistencies and anomalies in application information that indicate identity theft or other types of fraud.

Authoricheck[SM]: A class-leading business fraud prevention tool, Authoricheck[SM] provides an efficient, automated method for managing risk and eliminating fraud in a business-to-business environment by authenticating information in business credit reports and checking against historical application data for fraud indicators.

Appendix B: Experian Case Studies

Leading credit card issuer reduces fraud losses through implementation of Experian's Authentication Services

A major national credit card issuer with approximately 45 million accounts, growing by about 10,000 accounts a day, faced a significant application fraud challenge. The company needed to reduce application fraud losses, improve business efficiency and maintain customer service satisfaction, and it needed to do so cost-effectively. The company turned to Experian for help.

It chose to implement Level One of Experian's Authentication Services. The first of three increasingly sophisticated Authentication Services levels, Level One is powered by a database of more than 215 million consumers and 25 million businesses.

The credit card issuer, consulting with Experian, conducted a six-month test on 800,000 new applications before implementing the fraud prevention tool across its business. Utilizing the Authentication Services Level One has resulted in a 13 percent decrease in application fraud losses and an overall annual savings of $18 million.

The company is now exploring application of the service for risk assessment in prescreen credit offers and has taken its fraud prevention efforts a step further by becoming a subscriber to Experian's National Fraud Database.

National telecommunications provider benefits from Experian fraud solutions

The wireless communications industry faces exorbitant fraud losses – an estimated $275 million in 2003 alone. A national wireless telecommunications provider, challenged by fraud losses and high customer acquisition costs, turned to Experian for

help. The company recognized the need to protect both consumers and the company from identity theft and needed an aggressive fraud prevention strategy that was both highly effective and easy to implement.

After carefully reviewing other options, the telecommunications provider chose to share its fraud records with other organizations as a member of Experian's National Fraud Database (NFD). The NFD is a database of known, confirmed fraud information shared by members from multiple industries including online retail, bank card issuers, credit card providers, automotive lenders and telecommunications companies. The NFD alerts participants to confirmed fraud data as they process applications.

The wireless telecommunications provider tested the database for almost a year before proceeding with national implementation on all of its new accounts. The company reduced its fraud losses per handset by 55 percent and decreased the time it took to confirm fraud records by 66 percent.

In addition to cost savings, the company is able to detect attempted fraud much faster, protecting consumers from identity theft. Members of the NFD are able to stop identity theft at the point of application, notify the intended victim before fraud happens and prevent any harm associated with the crime.

Statistical analysis of shared fraud information in the telecommunications, credit card and online retail industries has proven that identity thieves cross industry lines when committing fraud. Equally important, identity thieves demonstrate predictable patterns of fraudulent behavior. As a result, all of the participants in the NFD benefit from responsibly sharing of verified fraud data from their respective industries.

Appendix C: CDIA Consumer Fraud Victim Assistance Initiatives

In 2000, the Consumer Data Industry Association (CDIA), then the Associated Credit Bureaus (ACB), announced a series of initiatives to more efficiently and effectively assist consumers victimized by fraud or identity theft. Those initiatives included:

- Improving the effectiveness of credit report security alerts through computer-readable codes. The codes notify creditors of the existence of potential fraud and help them avoid opening additional fraudulent accounts even when an automated review system is used. CDIA and its members strongly advocate use of the coded security alert system among creditors and other credit report users.
- Implementing new victim-assistance best practices to provide more uniform processes for victims working with personnel from multiple fraud units.
- Sending notices to creditors and other credit report users when a consumer doesn't recognize a recent creditor inquiry on their report and fraud is suspected.
- Implementing automated telephone systems that when reached by a consumer automatically add a security alert to a victim's credit history, opt them out of prescreened credit offers, and mail a copy of their credit report within three business days.
- Monitoring a victim's credit history for three months after correcting and eliminating fraudulent information. The agencies notify the victim of any

unusual patterns or activity during that time and provide fraud unit contact information.

- Launching new consumer education programs to help people understand how to prevent identity theft and what steps to take if they are victimized.

Most recently, Experian and the other national credit reporting agencies, working with the Federal Trade Commission, launched a new service eliminating the need for consumers to make multiple calls to have security alerts added to their credit history. Consumers now must call only contact one of the national agencies, in Experian's case, either by telephone or through its Web site. Their request will be forwarded to the other two and security alerts will be added automatically to all three of the person's credit histories.

Appendix D: Experian's Consumer Fraud Victim Assistance Process

STEP 1: Consumer contacts Experian's consumer assistance center

- Consumers can call Experian's automated voice attendant or logon to its Web site 24 hours a day, seven days each week, 365 days a year.
- A 90-day "Security Alert" is immediately added to the consumer's credit file. This alerts creditors to verify the identity of the consumer before extending credit.
- The consumer is put on the "opt-out" list for prescreened credit solicitations.
- The consumer is sent a complimentary consumer report within three business days.
- Experian's consumer education department developed and maintains a series of one-page educational fact sheets to help consumers better understand how credit reporting works and how to prevent ID theft or recover from victimization. In addition, Experian's Internet credit fraud center at www.experian.com provides a wealth of information to consumers and fraud victims.

STEP 2: Consumer receives report

- The consumer reviews his or her consumer disclosure for fraudulent data and calls a special telephone number listed on the credit report to speak with an Experian customer service representative specially trained in fraud victim assistance, or requests an investigation of any inaccurate information online.

- A seven-year "Victim Statement" can be added to the consumer's credit file if the report contains evidence of fraud. This asks lenders to contact the consumer by telephone before granting credit it his or her name.
- Together, the consumer and the customer service representative identify fraudulent items. Investigation, verification and removal of fraudulent items begin immediately. The creditors' addresses appear on the credit report to facilitate removal of the account information from the creditor's records.
- If a consumer elects to add the long-term victim statement, they are mailed two additional complimentary credit reports over a 90 day period enabling the consumer to monitor their credit history for additional fraudulent activity that may occur.

STEP 3: Investigation begins

- Experian notifies the creditors or data furnishers of alleged fraudulent items, typically through an immediate, automatic information transfer.
- Upon receipt of a valid police report Experian immediately blocks alleged fraudulent information from view by creditors and other users of the report. This allows a victim to continue to be credit active without being penalized for any fraudulent information on his or her report.
- Experian employs special system procedures and matching criteria to ensure that fraudulent data is removed as soon as possible.

- Experian attempts manual phone verifications and written proof documents from creditors, providing special services when appropriate for fraud victims to remove fraudulent data expeditiously.

STEP 4: Fraudulent data is removed

- Experian completes an investigation involving fraudulent information within 30 days. If the data contributor cannot verify information as accurate within the statutory deadlines, Experian's systems are designed to delete or update the information and prevent reappearance of the data.

NOT FOR PUBLICATION UNTIL RELEASED BY
HOUSE FINANCIAL SERVICES COMMITTEE
FINANCIAL INSTITUTIONS AND CONSUMER
CREDIT SUBCOMMITTEE

STATEMENT OF

COMMANDER FRANKLIN D. MELLOTT
MILITARY VICTIM ASSISTANCE COORDINATOR, IDENTITY THEFT RESOURCE CENTER

BEFORE THE

FINANCIAL INSTITUTIONS AND CONSUMER CREDIT SUBCOMMITTEE

OF THE

HOUSE COMMITTEE ON FINANCIAL SERVICES

ON

FIGHTING IDENTITY THEFT — THE ROLE OF FCRA

JUNE 24, 2003

NOT FOR PUBLICATION UNTIL RELEASED BY THE
HOUSE FINANCIAL SERVICES COMMITTEE
FINANCIAL INSTITUTIONS AND CONSUMER
CREDIT SUBCOMMITTEE

Mr. Chairman, Mr. Sanders, and other members of this subcommittee, please accept my thanks for inviting me to be part of this hearing today. I appreciate the opportunity to work with you in your efforts to combat the rapidly growing and even faster evolving crime of Identity Theft. The views I express today are my own and do necessarily represent the views of the Department of Defense or the Navy.

I am a victim of False Personation as defined by §529.3 of California Penal Code, and I am also the victim of Identity Theft as defined by the Identity Theft and Assumption Deterrence Act of 1998. Like nearly 40% of all identity theft victims, the perpetrator was a family member. In my case, the criminal was my estranged half-brother.

I discovered that I'd been victimized when, in the summer of 2001, I received a letter from the Department of Treasury stating that my year 2000 Federal Income Tax refund of nearly $5000 was sent to the Child Support Division in the Orange County California District Attorney's Office. Worse yet, the same letter threatened to intercept "all Federal payments." Since my paycheck was a Federal payment, I had to face the possibility that in as little as ten days I would stop receiving my paychecks. The more I thought of the consequences of this letter, the more concerned I became. This could easily cause me to lose my security clearance, and that in turn would prevent me from promotions, prevent me from being selected to command a unit, lead to an IRS audit, and cause problems in all facets of my life. It endangered my ability to support my family.

This all started when my half-brother used just a single piece of my identity information, my Social Security Number (SSN), and established credit with Time Warner Cable of New York. When he failed to pay the bill, Time Warner reported the debt against me. It later showed up on my credit report as a collection action. In calendar year 2000, my half-brother again used my SSN; this time he used it on W-2 forms filed in California with Breckenridge Group Incorporated and Pep Boys Incorporated. I do not know if either company verified the identity information. Somehow, the Child Support Division of the Orange County California District Attorney's Office found out that my half-brother was working. Since he owed them more than $75,000 in back child support, they pulled data from employment records and forwarded it to the Federal agencies under a collection program. Unfortunately, they forwarded my SSN, since that's what came from the W-2s. They did this without first matching my brother's name to the SSN he provided -- which was mine.

Up until that moment, I had intended to spend my summer leave period spending quality time with my two boys after back-to-back sea tours and three overseas deployments. Instead I found myself fighting for my financial future and my Naval career. There was jurisdictional finger pointing just trying to get someone to take a police report. There were countless telephone calls and letters to credit reporting agencies. I spent more than 100 hours working with the IRS and two companies in California trying to resolve income wrongly reported against my taxpayer ID number. Generally speaking, I wasted my valuable time off from the rigors of combat duty fighting with a system that makes it all too easy for a criminal to get credit in someone else's name. The mess was entirely mine to clean up. Unfortunately, it got worse.

In February 2002, after I placed fraud alert on my accounts with all three reporting agencies, my half-brother was able to use my SSN yet again – this time establishing cellular service with

AT&T Wireless. To add insult to injury, after I filed my initial fraud notifications, Experian merged my credit history with that of the criminal! They listed his wife's name as my wife, put most of his previous addresses in my file, listed his name as an alias of mine, listed his SSN as an alternate SSN of mine, and listed numerous collection actions from his past on my otherwise spotless file. When I asked how it happened, I was told, "the computer did it." I wish I could say this was a singular event, but it was not. I also found the reporting agencies unresponsive. Just a few months ago, after my case was featured in SmartMoney Magazine, I sent all three credit reporting agencies a certified-return receipt letter asking them to incorporate specific wording in my fraud alert. I asked that if they could not (or would not) to inform me why. Not a single one of them incorporated the language. None of them even bothered to reply.

Not only did my half-brother's actions tarnish my good name and adversely affect my credit history, they might well have ended my 17-year Naval career. A substantial mistake by a credit-reporting agency could well have done the same. Clearance for and access to classified National Security Information, as defined by Executive Order 12958, is determined by, among other things, one's credit history. Because of the lessons learned in espionage cases of recent years, any blemish on one's record is sufficient cause to remove access to National Security information. Each time my half-brother committed identity theft using my information, he jeopardized my security clearance. When Experian merged my file with my half-brother's, their action only made my problems worse. Instead of having just one or two bad entries on my credit, I now had several more. The danger to my security clearance -- the danger to my livelihood -- was grave. As an active duty Naval officer, in my line of work, if I do not have a security clearance, I am useless. My performance is rated against my peers. Without a security clearance, I am unable to do my job and lose my ability to compete for promotion. Losing my clearance would end my career – just three years shy of retirement. Not only must I fight the effects of identity theft, but I must also fight the blunders made by the credit reporting industry.

While I am concerned about myself, I am even more concerned for those 19 year-old Soldiers, Sailors, and their families that are so easily victimized by this crime. Imagine their spouses, new to the ways of the military, trying to balance the day-to-day challenges of a young family with the crippling effects of identity theft and mistakes by the credit industry. Furthermore, I am concerned because I can see how it could be nearly impossible to fight these problems from overseas.

In the end I have managed to keep my name clear, but it has not been easy. Congresswoman Loretta Sanchez and her staff helped me at a key juncture. To her I owe my gratitude. After the run-around from three different law enforcement agencies over jurisdictional issues, Special Agent Chris Behe of the Naval Criminal Investigative Service deserves praise. He was the first one to see the threat this crime posed to military members and found a way for me to file a report. That report was the catalyst that ultimately led to my half-brother's arrest.

Our nation is at war. Like anyone else who wears the uniform, I can be deployed overseas without notice. Quite honestly, my family and I do not need the additional stress imposed on us by this crime. When such a crime is perpetrated against military members who are deployed overseas, it may be months before they even discover the crime. It could be even longer before they could do anything about it. My half-brother was using my SSN for well over a year before I discovered it.

Current statistics indicate that it takes an individual 175 hours and about $1400 out of pocket to fix the damage caused by this crime. How can we, as leaders, expect a young Soldier, Sailor, Marine, or Coast Guardsman to do this while serving in one of the many remote corners of the world, while running drills aboard a submerged ballistic missile submarine, or while patrolling a dark street in Baghdad? The simple answer is that they cannot. Yet their inability to act can mean financial ruin. As an officer, I feel we owe our Soldiers, Sailors, Marines, and Coast Guardsmen more. Quite honestly, you are paying all of us in uniform to do other things, and I would hope that it bothers you to see us so easily distracted by the effects of this crime.

Anything that you can do to make it more difficult to commit identity theft, anything you can do to hold accountable those agencies that carelessly extend credit without appropriate protections against fraud, and anything you can do to improve the accountability of the credit reporting agencies will be significant and well worth your effort. There are those who will contend that existing measures are sufficient or at most require only minor changes. To those people I would say to put their financial future on the table in support of their beliefs: call the toll-free numbers, place fraud alerts on their credit files, and then publish their name and SSN on the internet. If they are unwilling to trust the very measures they contend are sufficient, then I suppose one could rightfully ask "Why not?"

Mr. Chairman, that concludes my prepared remarks. I am eager to answer any questions that you or other members of the subcommittee may wish to direct to me.

Statement of Daniel L. Mihalko, Inspector in Charge
Congressional & Public Affairs
Of the
United States Postal Inspection Service
On Fighting Identity Theft
And the
Role of the Fair Credit Reporting Act

Before the
Financial Institutions and Consumer Credit Subcommittee
of the
Financial Services Committee
U.S. House of Representatives

June 24, 2003

Mr. Chairman and members of the Subcommittee: thank you for holding this hearing on the topic of identity theft, America's fastest growing crime. I appreciate the opportunity to discuss the subject of identity crimes and related fraud, and the role of the United States Postal Inspection Service in combating this rapidly growing menace.

Role of the Postal Inspection Service

The U.S. Postal Service delivers more than 200 billion pieces of mail a year, containing money, messages, and merchandise, to 138 million addresses at some of the most affordable postage rates in the world. U. S. Postal Inspectors are mandated to safeguard all of it—including the people who move it and the customers who use it.

Congress empowered the Postal Service "to investigate postal offenses and civil matters relating to the Postal Service." Through its security and enforcement functions, the Postal Inspection Service provides assurance to American businesses for the safe exchange of funds and securities through the U.S. Mail; to postal customers of the "sanctity of the seal" in transmitting correspondence and messages; and to postal employees of a safe work environment.

As one of our country's oldest federal law enforcement agencies, founded by Benjamin Franklin, the United States Postal Inspection Service has a long, proud and successful history of fighting criminals who attack our nation's postal system and misuse it to defraud, endanger, or otherwise threaten the American public.

Postal Inspectors work closely with U.S. Attorneys, other law enforcement agencies, and local prosecutors to investigate postal cases and prepare them for court. There are approximately 1,900 Postal Inspectors stationed throughout the United States who enforce roughly 200 federal laws covering investigations of crimes that adversely affect or fraudulently use the U.S. mail and postal system.

Last year, U.S. Postal Inspectors made more than 11,000 arrests, over 6,000 of which were related to mail theft. One-third of those 6,000 involved identity theft. In the first eight months of our 2003 fiscal year, we have already exceeded the number of identity theft arrests made throughout all of last year.

What is Identity Theft?

Identity theft occurs when a thief steals key pieces of someone's identifying information, such as name, date of birth, and Social Security number, and uses the information to fraudulently apply for credit or to take over a victim's credit or bank accounts. Identity theft occurs in a variety of ways. Those that involve the use of the mail receive swift and aggressive action by Postal Inspectors. We ensure that consumers are being protected. In addition, we work with the mailing industry to develop best practices on how best to design mailing pieces to prevent identity theft. Our collaboration with the mailing industry is another example of how the industry as a whole is serious about the issue and working to stay on top of it for the benefit of consumers. Mail is important to consumers who receive it and to the businesses that send it.

Tactics Used by Identity Thieves

In the past, pre-screened credit solicitations were more vulnerable to identity theft because they simply required the customer to sign the solicitation and return it. When the items were stolen from the mail, they presented a risk to the consumer. But now credit card companies have begun automatically discarding such applications when they are returned with a change of address. Actions by the industry have made these mailings less attractive to the identity thief.

Identity theft is continuing to evolve with the expansion of the Internet and other electronic means. The mail is no more vulnerable than other sources of personal information, such as corporate and government records and computer databases. Financial institutions have implemented many safeguards to reduce the likelihood that personal financial information found within the mail can be stolen. The Postal Service is continually working to improve the security of the mail, and Postal Inspectors are making great strides in apprehending those who would use the mail to further their crimes.

Identity fraud is digging deep into consumer's pockets -- millions of dollars were lost in the past year by financial institutions and victims across the country. Thieves use a variety of tactics to drain a victim's finances, including stealing mail; posing as a loan officer and ordering your credit report (which lists account numbers); "shoulder surfing" at the ATM or phone booth to get your PIN code; and "dumpster diving" in trash bins looking for credit applications, canceled checks or other bank records.

Until a few years ago, a thief could submit an address change to divert customers' mail without their knowledge. Usually, redirected mail is sent to a commercial mail receiving agency in an attempt to ensure the perpetrator's anonymity. In response to recommendations by the Chief Postal Inspector, a prevention measure that addresses fraudulent change-of-address orders was adopted by the U.S. Postal Service. Post Offices now send a "Move Validation Letter" to both the old and new address when a change is filed. The letter instructs an individual to call an "800" number if a change was not filed. This simple measure has virtually eliminated the use of placing a false change-of-address order with the Postal Service as an avenue for committing identity theft.

Impact on Victims

One of the most insidious aspects of identity theft is the length of time the scheme is carried out before it comes to anyone's attention. It may be months before a victim realizes they've been targeted. It's not until a consumer gets turned down for credit, a car loan, or a mortgage on a dream house because of a bad credit rating—knowing they've paid their bills—do they begin to realize what has taken place. Most victims do not learn about the theft of their identity until 14 months after it has occurred. More than half of the victims we interviewed report their cases have been open, on average, 44 months. They also reported that, as victims, they spent, on average, 175 hours actively trying to restore their credit and "to clear their good name."

Identity theft can do more than ruin a person's credit; it can cause more serious damage. Identity theft hurts a victim in two ways. At first a victim must deal with the obvious financial issues. The second, hidden, factor is the emotional one: having to deal with privacy and practical issues such as a credit history that isn't theirs. The problem doesn't go away with a few phone calls -- it can stick with a victim for a long time. That's why it's such a serious issue. Victims run the gamut of society, they're wealthy, they're poor, they're old, and they're young. Anyone can become a victim.

In a recent Postal Inspection Service investigation based in Chicago, Illinois, the destructive activities of an identity thief resulted in the loss of thousands of dollars and the death of a primary victim. This scheme began in July 1999 when the identity thief began dating the estranged wife of a Chicago resident. Without his knowledge, the wife assisted the thief in stealing her former spouse's identity by providing the thief with the spouse's personal information.

In January 2000, the spouse filed a complaint with the Chicago Police Department after realizing that he was a victim of identity theft with losses exceeding $200,000. In February, the spouse received a package from the thief wrapped as a FedEx delivery. After holding the package for several days, the spouse received a voice mail message from the thief indicating the package was a gift. As he sat in his living room, he opened the package, which exploded, killing him instantly.

Last year a colleague of mine learned about identity theft the hard way. His bank called him in April last year and asked if he had authorized a $4,500 cash advance on his credit card in Miami, Florida that day.

He was stunned. The bank had called only hours after the withdrawal was made, following an alert initiated because certain account parameters indicated something might be wrong. Luckily for him, the bank simply asked that he sign an affidavit that he had not been in Miami and hadn't made the withdrawal. He wasn't held liable for the money. And he never found out what ID the thief had used to get access to his account.

Unfortunately, my colleague's ordeal wasn't over. He received a call a few months later from a cellular phone company, asking if he'd opened an account with them in Miami. Someone had racked up $1,800 in calling charges under his name and then disappeared. Once again, he signed an affidavit disclaiming knowledge of the charges, and the account was cleared. This time, he called the three main credit bureaus and reported the fraud.

My colleague is just one of hundreds of thousands of individuals who are victimized each year. The culprits may be found among employees (or patrons) of mailrooms, airlines, hotels or personnel offices--anyone who has access to a person's financial information. They can use your credit card or instead use encoding equipment, sold by business supply companies, and blank cards with magnetic strips on the back, to encode your account number onto a counterfeit card with a different name. Thieves sometimes seek jobs specifically to get access to financial information; alternately, they may bribe employees in such positions to supply them with the data they want.

The problem is compounded by the ease with which a phony ID can be obtained. On the Web are scores of sites with complete instructions on creating a "new you." Personal computers, "scanners" and color printers (or copiers), all facilitate creating false identification documents.

Commitment of Resources and Jurisdiction

Because identity theft crimes can involve the use of the mail, the U.S. Postal Inspection Service has become a lead agency in investigating these crimes. Even in cases where the original theft does not involve the mail, the mails may used to send the credit cards to a commercial mail receiving agency or alternate

address. That's why Postal Inspectors are involved in investigating this crime and take it so seriously.

Each of the Inspection Service's 18 field divisions investigates identity theft within their respective boundaries. Identity theft investigations are reported, categorized, and tracked in an Inspection Service national database used by management to coordinate the appropriate investigative response. During the past few years, Inspection Service resources devoted to identity theft investigations have increased significantly – by 38 per cent.

As the resource commitment increases, so have the number of arrests. In 2001, we made 2,097 arrests; in 2002, 2,243. As of May of this year, we've made 2,264 identity theft arrests. Keep in mind this is in the context of 200 billion pieces of mail the Postal Service handles annually. But we take this crime seriously because of the impact on its victims. Due to our efforts, the mail may be one of the most protected mediums where identity theft is investigated and prosecuted.

Identity Theft Investigations

In a typical case this year, Postal Inspectors arrested eight West African nationals who were operating a multimillion-dollar counterfeit and stolen credit card enterprise nationwide. And Postal Inspectors in New York arrested 16 members of a gang that ran a passport photo business, supplying false identifications for cashing checks stolen from the mail.

Last week Postal Inspectors announced the results of a round-up of 103 mail thieves throughout the western United States. A multi-agency task force comprising U.S. Postal Inspectors, members of the U.S. Marshals Fugitive Apprehension Strike Task Force, U.S. Secret Service, state and local police, and the Northern California Identity Theft Task Force targeted mail thieves in California and Nevada. Similar operations took place in Arizona, Hawaii, Utah and New Mexico. Federal and state prosecutors are supporting the work of the task force by aggressively prosecuting individuals involved in mail and identity theft.

Here are just a few examples of identity theft cases investigated by Postal Inspectors in the past year. In Detroit, Postal Inspectors investigated a gang of mail theft recidivists who were recruiting street people, called "runners," to obtain cash advances from banks and casinos via credit cards. Inspectors executed a search warrant at the residence of a suspect in January 2002 and recovered more than 180 documents listing victims' personal IDs. Inspectors and agents from the Detroit Metro Identity Theft Task Force identified and arrested the ringleader of the group who, at the time of his arrest, had more than 700 car rental applications with names, dates of birth, Social Security numbers, and credit card accounts of potential victims. The ringleader and a cohort reportedly called credit card issuers, purporting to be the true account holders, and requested that replacement credit cards be mailed to them. The car rental manager who supplied the rental applications and an employee who worked at a

health plan office were later indicted for providing documents to the gang. Total fraud losses exceeded $700,000.

An Illinois man was sentenced last year to 25 months in prison and ordered to forfeit $590,000 in assets to banks after pleading guilty to the unlawful possession of an access device, mail fraud, and bank fraud. A joint investigation by Postal Inspectors and special agents of the Social Security Administration determined he had fraudulently applied for more than 200 credit cards using numerous victim IDs.

Postal Inspectors in Jacksonville, Florida, arrested six people believed to be running a major identity theft ring. The arrests were the result of a joint investigation by the Northeast Florida High Tech Task Force, which includes Postal Inspectors, members of the Jacksonville Sheriff's Office, and several other federal, state, and local law enforcement agencies. Victims of the ring included employees of the Winn-Dixie Corporation and Hollywood, Florida, police and fire departments. The six suspects were charged with 44 counts of violations related to the Racketeering Influenced Corrupt Organization (RICO) Act, including criminal use of personal information, grand theft, organized fraud, and manufacturing fraudulent IDs. On May 27, 2002, one of the suspects pled guilty to RICO violations and related charges.

Las Vegas police arrested a man last year for "driving under the influence" and later discovered he had an outstanding arrest warrant for identity theft in Arizona. Phoenix Postal Inspectors reported he stole a person's Social Security number, applied for numerous credit cards in the victim's name, and had the cards mailed to a box he rented at a commercial mail receiving agency. Postal Inspectors and Secret Service agents searched the man's business and discovered numerous fraudulent documents.

Statutes Used in Identity Theft Cases

A number of statutes enable us to take action against identity theft involving the use of the mail. Under Title 18, U.S. Code, Section 1708, Postal Inspectors may arrest individuals for the possession of stolen mail or filing a false change-of-address order; the penalty is a $2,000 fine or up to five years' imprisonment, or both. In 1998, the Identity Theft and Assumption Deterrence Act of 1998, was signed into law. This law expanded the scope of the identity fraud statute (18 U.S.C. § 1028), and made it a federal crime for the unauthorized use of personal identification in the commission of any federal law (felony or misdemeanor), or a state or local felony.

But one of our top weapons in the fight against identity theft is a statute originally enacted over 125 years ago: the criminal mail fraud statute. If someone applies for a credit card in your name, perpetrators may be prosecuted under Title 18, USC 1341. The penalty is a $1,000 fine or up to five years' imprisonment, or both--unless a financial institution is affected, in which case the fine may be raised to $1 million and imprisonment for up to 30 years. The public policy that underlies this statute remains valid today: *The postal system created by*

Congress to serve the American public should not be used to conduct schemes that seek to cheat the public.

Our experience demonstrates that enforcement laws, coupled with an aggressive education campaign, industry cooperation, interagency enforcement efforts and preventive/security measures described below, are invaluable tools in the arsenal of law enforcement.

Interagency and Industry Cooperation

To address the fundamentals of identity theft, the Postal Inspection Service works diligently with the credit card industry, financial institutions and other law enforcement and regulatory agencies. In 1992, the Postal Inspection Service sponsored its first Credit Card Mail Security Initiative meeting in Washington, DC. We continue to promote and host these semi-annual meetings.

Many of the preventive strategies discussed at our meetings have been implemented by our financial industry partners, and have resulted in reduced losses attributed to mail theft and the subsequent identity theft that occurs from it. The now-common concept of credit card activation was first proposed by a Postal Inspector and was promoted through the Credit Card Mail Security Initiative meetings. The industry embraced and implemented this prevention strategy, which resulted in the reduction of significant industry fraud losses over the past decade.

In addition, working in conjunction with industry partners, Postal Inspectors analyze information from credit card thefts to identify "Hot Spots" for investigative attention. The Postal Inspection Service notifies the financial industry of zip code areas suffering abnormal losses, so they can take extra precautions when mailing to those areas.

Thanks to the collaborative efforts between the Postal Inspection Service and its working-group partners, we are beginning to see the results of this and many other fraud prevention initiatives. In addition to modifying industry practices, our collaboration has produced a number of fraud prevention guides, including the Fraud Detection and Reference Guide; Account Takeover Prevention Guide; and Detecting and Preventing Credit Application Fraud. The working group was also responsible for the Identity Theft Consumer Awareness video and the Identity Theft brochure. At the conclusion of my testimony, I have included prevention tips prepared by the Postal Inspection Service in collaboration with its working partners.

In 2003, the Postal Inspection Service decided to broaden the scope of the Credit Card Mail Security meetings to include presentations on money laundering, Internet fraud, and bank fraud schemes. As the focus has expanded, the name of our working group has changed to the Financial Industry Mail Security Initiative (FIMSI). The initiative has decided to capture many of the best practices

developed over the years and share them with industry and law enforcement in the form of a report that will be published this year.

To manage the vast data associated with these crimes, the Postal Inspection Service has developed a new financial crimes database. This computer application compiles a myriad of intelligence data relating to financial crimes, and provides Postal Inspectors with information that assists in identifying trends, criminal hotspots, and the scope of identity theft activity. Information for this database is provided by credit card issuers, other financial institutions, mail order companies, Postal Inspection Service investigations, and the victims themselves.

Task Force Efforts

In addition to partnering with members of the financial and mailing industry, task force efforts by law enforcement have been a successful approach to the identity theft issue. Postal Inspectors are active participants on financial crimes task forces throughout the nation. In Pittsburgh, Pennsylvania, the Postal Inspection Service leads the Financial Crimes Task Force of Southwestern Pennsylvania. This task force began operation on January 17, 1995, and is housed at the Pittsburgh office of the Postal Inspection Service. Originally, this task force was formed to target major credit card fraud in the Pittsburgh area. However, with the increased number of instances of identity theft spreading rapidly throughout America, this taskforce has directed most of its resources toward identity theft investigations.

One of the recent cases involved actor Will Smith as a victim of identity theft. When Smith played Agent J in the movie Men in Black that was showbiz. But when convicted felon Carlos Lomax impersonated actor Will Smith, that was identity theft. Will Smith never knew his identity had been stolen until he attempted to purchase a new home and found his credit had been compromised. Postal Inspectors and the Financial Crimes Task Force of Southwestern Pennsylvania arrested Lomax for identity theft, and Lomax was sentenced to serve 37 months in jail and pay $64,000 in restitution.

The Minnesota Financial Crimes Task Force, which includes Postal Inspectors, Secret Service agents, and local law enforcement officers, last year arrested a Nigerian national for a $1 million account-takeover scheme. Postal Inspectors executed a federal search warrant at the suspect's residence and recovered approximately $16,000 in cash, three vehicles, artwork, electronics equipment, and merchandise derived from the scheme. An investigation revealed the man used bank employees to identify high-dollar, dormant accounts with balances of $100,000 or greater for his scheme, and shipped the fraudulently obtained merchandise to his home in Nigeria.

Public Awareness and Education Efforts

Over 2,000 of our 6,000 mail theft arrests last year involved identity theft -- and it's getting worse. But arrests are not the only solution. That is why the Postal

Inspection Service addresses the identity theft issue on two levels -- aggressive investigative efforts and creating prevention and awareness programs.

While the Postal Inspection Service works hard to identify and prosecute identity crimes, we also recognize our ability to lessen the impact of this crime upon the public through various prevention campaigns. Postal Inspection Service efforts to prevent identity theft target the public and business communities to educate them about these schemes, and the problems associated with them. These efforts have included the publication of a brochure titled, *Identity Theft, Safeguard Your Personal Information,* and the March 2000 release of the Showtime movie, *The Inspectors 2,* based on Postal Inspection Service files relating to identity theft investigations.

In an effort to educate consumers about this fast-growing crime, the Postal Inspection Service created an informational video titled *Identity Theft: The Game of the Name*. Also, the Postal Inspection Service and the Postal Service's Consumer Advocate Office partnered during this year's National Consumer Protection Week, from February 3 through 8. The week's theme was "Identity theft, the No.1 consumer fraud in the nation."

In 1999, Postal Inspectors along with partner organizations undertook Project kNOw Fraud, which was the largest consumer awareness campaign undertaken in this country. Through a mailing to 123 million addresses we warned the public of the dangers of telemarketing fraud. The successful campaign was followed up with the National Fraud Against Seniors Awareness Week in August of 2002. In September of this year Postal Inspectors will be unveiling another national awareness campaign. This year's topic is identity theft.

Actor Jerry Orbach, who also was a victim of identity theft, will be the campaign's spokesman. This awareness campaign features a two-pronged approach, providing prevention and awareness information to consumers and addressing businesses on the need to safeguard there files and databases of customers' personal information. The campaign will include:

- A house-to-house mailing to residences in ten states identified by the FTC as reporting the most identity theft complaints. The ten states are California, New York, Texas, Florida, Illinois, Pennsylvania, Georgia, Michigan, New Jersey, and Arkansas. The mailing will be made the first of September in conjunction with a planned press conference.

- Distribution of an updated brochure on identity theft. The brochure will be distributed in connection with identity theft presentations made by Postal Inspectors to consumer groups.

- Production and release of a Public Service Announcement (PSA) featuring actor Jerry Orbach. This thirty-second PSA will be released in September in conjunction with a press conference.

- An identity theft insert outlining prevention tips that will be included with monthly financial industry statements and with all Stamps by Mail orders placed during the months of September, October, and November.

- Production of an identity theft poster that includes prevention tips that will be displayed in all Postal Service retail lobbies, numerous credit unions, financial institutions, and police departments in September.

- Production of an identity theft informational video and articles on identity theft prevention for publication in internal and external publications as well as running newspaper ads in the same ten states that have been identified as reporting the most complaints.

The Mullen agency of Pittsburgh has provided support for this campaign on a pro bono basis. But what really makes this campaign unique is the funding source. We've all heard the saying, "crime doesn't pay." In the case of this awareness campaign, it does pay. This campaign is being funded through fines and forfeitures paid by criminals in a past fraud case.

Prevention Tips

In numerous formats, including our website at www.usps.com/postalinspectors, we provide the following recommendations to the public:

- Deposit your outgoing mail in a blue Postal Service collection box and promptly remove mail from your mailbox after delivery.

- Shred unneeded documents that contain personal information before discarding them.

- Order credit reports *every year* from each of the three major credit reporting agencies and thoroughly review them for accuracy.

- *Never* give personal or financial information over the telephone or the Internet unless *you* initiated the contact and trust them.

- Report lost or stolen credit cards immediately.

- If you applied for a credit card and didn't receive it when expected, call the financial institution.

- Sign new credit cards immediately--before someone else does.

- Memorize your Social Security number and passwords. Don't use your date of birth as your password and don't record passwords on papers you carry with you.
- Never leave transaction receipts at ATM machines, on counters at financial institutions, or at gasoline pumps.
- Don't carry your Social Security card or birth certificate; leave them in a secure location.
- Don't disclose credit card or other financial account numbers on a Web site *unless* the site offers a secure transaction.
- Closely monitor the expiration dates on your credit cards and contact the issuer if you don't receive a replacement prior to the expiration date.
- Beware of mail or telephone solicitations that offer prizes or awards--especially if the offer asks you for personal information or financial account numbers.
- Match your credit card receipts against your monthly bills and check your monthly financial statements for accuracy.
- Watch for your monthly financial statements and bills. If you don't get them when expected, contact the sender.

For victims of identity theft, we recommend the following initial steps to begin the long and arduous task of responding to the crime:

1. If the crime involved the U.S. Mail, contact your nearest U.S. Postal Inspection Service office and report it.
2. Call the fraud units of the three major credit bureaus and request a "fraud alert" be placed on your credit file. Check your monthly financial statements for accuracy.
3. Order copies of your credit report from the credit bureaus to check whether any fraudulent accounts were opened without your knowledge or consent.
4. Contact your banks and creditors, by phone and in writing, and report the crime. You may be advised to close some or all of your accounts. At the least, change your PIN codes and passwords immediately.
5. Record the names and phone numbers of people with whom you discussed your case and retain all original reports and supporting documents. Keeping accurate and complete records are a big step toward helping you resolve your problem.

6. Contact your financial institutions and request they flag your accounts. Instruct them to contact you immediately if there is unusual activity on your accounts.

7. File your complaint online with the Federal Trade Commission, or call their Identity Theft Hotline at 1-877-IDTHEFT. The FTC has counselors to assist identity theft victims with resolving financial and other problems that can result from this crime.

Educating the public and working to reduce the opportunities where the U.S. Postal Service can be used for illegal purposes are crucial elements in our fight against identity theft crimes. As always, we will do our part to remove criminals from society. We appreciate your recognition of the importance of this issue.

Testimony: Subcommittee on Financial Institutions and Consumer Credit
June 24, 2003
Testimony of Maureen V. Mitchell

Committee on Financial Services
2129 Rayburn House Office Building
Washington, D.C. 20515

Subcommittee on Financial Institutions and Consumer Credit
"Fighting Identity Theft ~ The Role of FCRA"

Statement of Maureen V. Mitchell: Ohio Identity Theft Victim

Mr. Chairman, Members of the Committee, my name is Maureen Mitchell and it is a privilege to have been invited to submit this testimony.

I am 47 years old, my husband Ray and I have been married for 26 years. We have a daughter in medical school and a son in college. I was born and raised in Woodside, New York. I was educated at Stuyvesant H.S. and Hunter College, CUNY. We have resided in Ohio since 1978. I am a Registered Nurse, and have been a licensed Realtor for 23 years.

My husband and I have always been financially prudent and fiscally responsible. We have always paid our bills in a timely manner, and we manage our finances prudently and responsibly. We have always exercised the normal consumer precautions to ensure our privileged financial information remains private. We have never lost our wallets, never been burglarized, we obtain the credit card receipts when we use our credit cards, we do not give our credit cards to waiters in restaurants, we do not bank on the Internet, we don't order merchandise via the Internet, and we shred our paper trash to prevent someone from "dumpster diving" and obtaining our personal information. We have never given our social security numbers out over the phone, and we had our social security numbers removed from our driver's licenses. We had also checked our credit reports in March of 1999 to ensure their accuracy.

In spite of all of the consumer precautions we have taken, we have become the unfortunate victims of Identity Theft. And, we were not only victimized once, we were victimized twice.

We first became aware of a fraud problem on September 12, 1999, when we received a phone call at home from a KeyBank service representative. Our KeyBank issued MasterCard account number was compromised and used by criminals to place fraudulent mail order purchases. We had never lost our credit cards, yet criminals somehow obtained our credit card account number and made fraudulent phone order purchases from an Illinois department store. The KeyBank service representative was calling because of an "unusual pattern of activity" on our credit card account. After much discussion, it was finally established with the service center representative that we

had not made or authorized the fraudulent charges. The service representative told me that KeyBank required us to report our credit cards as "lost or stolen". We objected to reporting our cards lost or stolen: my husband had his credit card in his wallet, and I had my credit card in my wallet. We were not given the option of closing the account at the request of the consumer due to fraudulent usage. Our credit card account was closed and we were to be issued new credit cards with a different account number. KeyBank never advised us to place Fraud Alerts on our credit reports, and said filing a police report was optional. I did file a police report with our local police department, and KeyBank launched an investigation. If KeyBank would have advised us to place Fraud Alerts on our credit reports, the following events may not have occurred.

On November 15, 1999 we received a phone call from JC Penney's credit department informing us that someone had used my husband's name and social security number to open an account at the JC Penney store at the Woodfield Mall in Schaumberg, Illinois. JC Penney became aware that the application was fraudulent when the bill was sent to the address given by the criminals on the fraudulent application. The bill was returned by the post office stamped saying "no such house number exists". The inability to deliver the bill was what prompted JC Penney to contact us. I informed the JC Penney representative of our KeyBank MasterCard account fraud, and was then advised by the JC Penney representative to contact the three major credit reporting agencies to place fraud alerts on our credit reports. I immediately called Trans Union, Experian and Equifax and placed the fraud alerts on our credit reports. Upon contacting Trans Union, Experian and Equifax, I was appalled to discover that we had been plunged into Identity Theft hell.

In speaking with Trans Union representative, I learned there had been 25 inquiries into our Trans Union credit report between September and November 1999. None of these inquiries were initiated by us legitimately seeking credit. I told the representative at Trans Union that there had not been 25 inquiries into our credit in the previous twenty years, and questioned whether that many inquiries in such a short period of time sent up "red flags' to Trans Union. The reply I received from the Trans Union representative was that it was not their job to monitor the number of inquiries, and it was suggested that I call all the merchants who made the inquiries. Trans Union provided me with the names and phone numbers of the merchants to contact. The list was extensive and included numerous car dealerships, banks, credit card companies, furniture stores, department stores and communication service providers. Trans Union did place Fraud Alerts on our credit reports at this time. I also contacted Experian and Equifax and was dismayed to learn that they too showed numerous inquiries into our credit reports during the same 60 day period.

In speaking with the credit reporting agencies I also learned that aside from an excessive number of credit inquiries into our credit reports, our credit reports now also contained numerous address changes. These address changes were entered into our credit reports without any verification of their accuracy. We've resided at the same address in Ohio for twenty years, yet our credit reports now showed us living at six different addresses in Illinois.

It seems rather incomprehensible that our previously impeccable credit reports, which clearly showed wise and careful use of credit along with a stable twenty year residence history, now showed over twenty five unauthorized credit inquiries and six out-of-state address changes, all of which had been entered on our credit reports between September and November of 1999. Had the merchants or credit reporting agencies contacted us by phone or mail to notify us that a credit application had been submitted using our names and SSN's but the address on the application did not match our address of record, much of the criminal activity would have been "nipped in the bud". An address discrepancy between a credit application and the address of record on a credit report should not be ignored by the merchants or the credit reporting agencies, identity thieves often use a phony address and phone number. It is imperative that a system of "checks and balances" be implemented and adhered with by the merchants and the credit reporting agencies. Credit bureaus must verify the accuracy of the information received prior to posting information on credit reports. The credit reporting agencies can use available technology to "red- flag" information that does not fit the profile of the consumers' previous spending habits. Change of addresses need to be verified by the credit reporting agencies prior to changing the address on the consumers' credit report. The information sold and disseminated by the credit reporting agencies to the various lenders and merchants making credit inquiries is perceived by these banks and merchants as accurate because "it came from the credit bureau". It seems incongruous to have banks and merchants rely on the information appearing on credit reports when this information has been entered without any verification of its accuracy.

As our ID Theft saga continued, I filed additional police reports, and I followed the advice of the Trans Union fraud representative and attempted to make phone contact with all of the merchants who appeared on the inquiry page of our credit reports. These efforts were extensive, time consuming and extremely frustrating. I was placing phone calls to these merchants in an attempt to "put them on notice" that we had not applied for any credit. Many times these phone calls were only answered by automated phone prompt systems that never offered me the option of pressing an extension to speak to a human being. I was often asked by the phone prompt to enter an account number. I did not have the account number because I was not the one who opened the account. I did make efforts to try to circumvent the automated phone prompts. I pretended I was calling from a rotary phone, which led me into a voice response automated prompt system, and I pressed zero hoping a "live person" would come on the line. These efforts were frustrating, time consuming, and often futile.

I also placed numerous calls to various state and federal agencies as I attempted to weave my way through the maze of credit fraud and Identity Theft. The office of the Ohio Attorney General suggested that I contact the Federal Trade Commission (FTC). My call to the FTC led me to their ID Theft Clearinghouse (877 438 4338). Kathleen Lund was the Identity Theft counselor with whom I spoke. Kathleen confirmed, based on the facts that I gave her, that we were victims of Identity Theft. Kathleen informed me of Title 18 Section 1028 of the US Code which made Identity Theft a federal offense. Kathleen provided me with invaluable information, guidance and emotional support

during this extraordinarily stressful time. It was a pleasure to finally speak with someone who had a clear and thorough knowledge of credit fraud and Identity Theft. It was also a great relief to finally speak to a human being after the automated answering prompt hell I had endured as I attempted to contact the merchants. Kathleen started a file on our ID Theft case and gave me the assigned file reference number to include in our police reports. She advised me to contact the SSA and the BMV to report the fraudulent use of my husband's SSN. Kathleen advised me to keep a running log of all calls and contacts relative to our ID Theft nightmare, and asked me to keep her informed of any new developments. Kathleen's assistance, guidance and advice were very helpful. However, it is the Identity Theft victim who bears the burden of the Herculean task of trying to clear their good name and restore their good credit.

As I continued my efforts to contact the merchants, I received three very alarming phone calls. The date was now November 18, 1999, three days after we placed the Fraud Alerts on our credit reports. The first call was from Citibank in Illinois alerting us that a twenty five thousand dollar ($25,000.00) personal loan application had just been made by someone using my husband's name and social security number. The loan application had been made in person by an impostor posing as my husband. This impostor had presented legitimate looking identification. Our credit reports were pulled as the loan officer was processing the loan application, and we were contacted because of the Fraud Alerts on our credit reports. I spoke to the fraud department of Citibank and explained that we had placed the Fraud Alerts on our credit reports three days prior when we became aware we were victims of Identity Theft. Citibank's fraud department said they would contact their security department, check to see if the impostor was on their surveillance tape, and call me back.

As I was waiting for the return phone call from Citibank, I received another alarming phone call. Thomas Retkowski, a fraud investigator from Bank One's regional fraud office in Wisconsin, called to inform us that a fifteen thousand dollar ($15,000.00) personal loan application had just been made in Illinois by someone using my husband's name and SSN... The Fraud Alerts on our credit reports prompted Thomas to call. I informed Thomas of the call I had received from Citibank just minutes before his call, and told him we were victims of Identity Theft. Thomas faxed us an affidavit to sign and have witnessed. I told Thomas we had filed police reports and had been in contact with the FTC. Thomas wanted us to immediately fax the signed affidavit back to him in Wisconsin. As the faxes were being sent, another call came in. Marquette Bank in Illinois had just received a five thousand ($5,000.000) loan application from someone using my husband's name and SSN. I told the fraud investigator from Marquette Bank about the two other fraudulent loan applications and the affidavit we were in the process of faxing to Thomas Retkowski.

Three different banks, all within close geographic proximity to each other in the greater Chicago area, had just received three fraudulent personal loan applications for varying amounts of money by an impostor using my husband's name and SSN. These fraudulent loan applications were all made in less than a two hour time period and they totaled forty-five thousand dollars ($45,000.00). The impostor had come into each bank,

sat down with a loan officer, filled out the necessary paperwork, presented legitimate looking photo identification as "Raymond Mitchell", and told each loan officer that he would come back to the bank to pick up "his" money in about an hour.

Thomas Retkowski received our signed fraud affidavit at his office in Wisconsin as I was contacting our Ohio police department to report that an impostor was currently applying for loans in my husband's name in Illinois. Aside from the emotional and psychological trauma we were enduring as victims of ID Theft, we now found ourselves embroiled in a very tension filled, time constraint driven drama that was unfolding before our eyes. We were dealing with three different banks in Illinois, communicating with a fraud investigator in Wisconsin, and filing an Ohio police report. To complicate matters further, we were dealing with two different time zones and we had a one hour window of opportunity before the impostor returned to the bank to pick up "his" money.

Thomas Retkowski's fraud investigation expertise and initiative synchronized well with the outstanding police cooperation we received from Chief Edward Matty and Sgt. Robert Verdi of our local Ohio police department. As a result of their coordinated efforts, plainclothes detectives from Lansing Illinois were in place at Bank One within the hour, awaiting the arrival of the impostor. The impostor returned to Bank One to pick up "his" money and was arrested as he exited Bank One after having fraudulently obtained the fifteen thousand dollars ($15,000.00). The impostor had five thousand dollars ($5,000.00) in cash and two five thousand dollar bank checks ($10,000.00) made payable to Raymond Mitchell. The money was recovered when the impostor was arrested. I was told by the arresting detectives that the impostor also had an Illinois driver's license and an Illinois State Identification Card, which displayed the impostor's picture along with my husband's name and SSN.

The detectives ran the fingerprints of the impostor, and discovered the impostor had 17 aliases and a twenty three year criminal history. A preliminary hearing was set for November 20, 1999, and the detective said he would keep me informed of any developments.

_____I continued to make phone calls to try to resolve this nightmare when I learned that the impostor was released on a signature bond in his own recognizance at the preliminary hearing. Words can't even begin to describe the horror I felt knowing that a suspect with seventeen aliases, multiple priors and an extensive criminal background was released on a signature bond in his own recognizance. The hearing was in Cook County, Illinois and the Judge was Thomas Panicki. I was also told that when this suspect was arrested he had stated to the detectives: "I didn't use a gun, I didn't use a knife, call my lawyer I will plead guilty and they will put me on probation".

It was appalling for me to realize the criminals commit these crimes with a premeditated methodology that accomplishes their criminal intent with the least possible risk for the criminal, if apprehended, serving jail time. These criminals are still committing bank robbery, fraud, identity theft, forgery and a litany of other criminal acts, however, since a traditional weapon was not used, the criminals, if apprehended, are

counting on probation instead of incarceration. The criminal misuse of technology that allows these impostors to fraudulently manufacture the documents necessary to steal the identity of another should be classified as a weapon, as serious a weapon as a gun or a knife. The criminal misuse of technology has become the Identity Theft impostor's weapon of choice.

The scales of justice are tipped in the wrong direction when an identity theft criminal is sentenced to serve a shorter period of incarceration than the length of time it takes the Identity Theft victim to clear their credit report and restore their good financial reputation! The jail sentences imposed on ID Theft criminals by state and federal courts need to be of sufficient duration to serve not only as a deterrent, but to truly reflect the egregiousness of these crimes.

As our Identity Theft saga continued, some of the cooperative merchants honored our requests and sent us copies of the fraudulent applications. These fraudulent applications contained numerous blatant errors that should have alerted the merchants and the banks that something was amiss. One example is an application that was made to purchase a Ford Expedition. This vehicle was purchased using my husband's name and SSN along with the name and SSN of a co-buyer. These two men presented themselves to the car dealership and said they resided together. However, on the application one man filled out his address as 2243 N.Grand and the other used 2243 W.Grand. On this same application, the phone number that was listed to verify place of employment had an area code of 300, this area code is not a valid area code in the continental United States. The criminals also purchased the 5 year 60,000 mile extended warranty which appeared on the application at a cost of $695.00. Yet, when this figure was carried over to the debit column to determine the amount of credit to be granted, the figure became $1695.00 instead of $695.00. The Raymond Mitchell impostor did not present a driver's license for identification; he used a janitorial services photo identification card. However, the signature on the janitorial services ID card did not match the criminal's signature on the loan application. And to top off the list of blatantly obvious errors on this application, our last name was misspelled! Our last name was not only misspelled on the loan application, it was also misspelled on the fax from the lender approving the loan. In spite of these GLARING "red flag" discrepancies, this loan was approved and these two men purchased a Ford Expedition using our credit history. Had this transaction been processed using due diligence and an iota of common sense these blatant discrepancies would have been caught. The possibility does exist that these criminals made the purchase through a car salesman, car dealership and lender that were co-conspirators, but I think that is a remote possibility. I do firmly believe that sloppy business practices substantially contribute to the criminal's ability to successfully defraud merchants and lenders. Shoddy business practices are abetting criminals in committing the crimes of credit fraud and Identity Theft, and plunging innocent victims into ID Theft hell. It was due diligence that was exercised by a salesperson in an Illinois furniture store that prevented the extension of credit when an impostor tried to purchase furniture. The salesperson realized that "something wasn't right" after reviewing the credit application. Credit was not extended by the furniture store and the criminal was thwarted in this

fraudulent attempt. I think this is a good example of how good business practices can diminish fraud.

In spite of the extensive time and effort we logged in trying to resolve this Identity Theft nightmare, we now had "derogatory accounts" appearing on our credit reports. We were also receiving phone calls from collection specialists. The Ford Expedition was not the only vehicle purchased by criminals using our credit history. We learned that a Lincoln Navigator had also been purchased by impostors when we received a phone call from a collection specialist who wanted to know why we were overdue on the payments for "our" Lincoln Navigator. I tried to nicely explain to these collection specialists that we were victims of Identity Theft and we did not purchase these vehicles or open the accounts they were calling about. I provided them with the name and phone number of the detectives, the police report number(s) and the reference number assigned by the FTC. I strongly suggested they not call me back unless they were willing to provide whatever information and documentation they might have to assist in the investigation. I always ended my conversation with the collection specialist by saying: "It's amazing to me that you can find the real Ray and Maureen Mitchell when you want to collect your money, too bad you didn't find the real Ray and Maureen. Mitchell before you loaned out the money."

We were able to determine from pictures we received from the car merchants that the criminals who purchased the vehicles were not the same person, and they were not the impostor who was apprehended leaving Bank One. We had been victimized by a sophisticated Identity Theft ring that operated in an organized and insidious manner.

The detectives told us that the criminals know when the fraud alerts on our credit reports will expire. The fraud alert was in place for two years, and if we failed to reactivate the fraud alerts our information would be re-circulated through the criminal ring again. Therefore, we will have to keep fraud alerts on our credit reports for the rest of our lives. So, in the future, when my husband and I apply for credit we will have to explain this nightmare to the lender, hope they believe us and hope they don't perceive us to be the criminals.

Our efforts to restore our good names and good credit history were extensive. I made hundreds of phone calls and I sent dozens of notarized, certified, return receipt requested letters to the merchants informing them that the applications they received were fraudulent. We submitted numerous affidavits, notarized statements and notarized handwriting samples. We filled out over twenty different sets of forms and documents in our attempt to comply with the merchant's requests for further information. The paperwork nightmare that we endured during our initial victimization was horrendous, and it added insult to injury. Seemed rather ironic that a criminal could fill out a fraudulent application, obtain credit in our names and easily have our address changed, yet, when we tried to dispute fraudulent accounts and have our address "corrected" back to our real address, we were inundated with paperwork requiring us to "prove" our identity and address.

A distressing and frustrating incongruity exists for victims of Identity Theft: the criminal is assumed innocent until proven guilty, but the Identity Theft victim is assumed guilty until proven innocent. The criminal can have a public defender appointed to protect his legal rights, however, if the Identity Theft victim needs to hire an attorney to assist in clearing their names and restoring their credit they will be paying substantial legal fees out of pocket.

We had exhausted all known resources in an effort to clear our names and restore our credit. I met with our Ohio Congressman, Steven LaTourette. It was through Congressman LaTourette's intervention and assistance that I was able to meet with the FBI. I met with numerous police officers. I met with a Victim's Assistance Program in Ohio and I contacted a Victim Advocacy Program in Illinois. I spoke to prosecuting attorneys, and sent packages of information to State's Attorneys. I begged, pleaded and cajoled to try and obtain a federal investigator and a United States' Attorney to take our case. The Lansing Illinois detectives who apprehended the Bank One impostor were limited to investigating crimes occurring within their jurisdiction. Identity Theft crimes are frequently cross-jurisdictional. Cooperation and coordination among federal, state, and local law enforcement agencies is of paramount importance to the successful investigation and prosecution of ID Theft cases.

I had frequent contact with Kathleen Lund, our ID Theft counselor at the FTC, as I attempted to continue to navigate my way through the labyrinth of Identity Theft hell. The input and support I received from her continued to be valuable and helpful. Kathleen asked for and obtained my consent to submit my name to be contacted by a member of the office staff of Senator Jon Kyl (R-AZ). Senator Kyl was going to chair an Identity Theft hearing, and wanted to have an Identity Theft victim testify at this hearing. I received a call from Jim McDermond, one of Senator Kyl's staff members. Jim requested information and documentation from me, which I gladly sent him. I was invited to testify at the hearing, which was held March 7, 2000. It was the Hearing before the Senate Committee on the Judiciary Subcommittee on Technology, Terrorism, and Government Information: "ID Theft: When Bad Things Happen to Your Good Name". It was my privilege to testify.

In my opinion, many good things were accomplished as a direct result of that hearing. Chairman Jon Kyl exhibited a sincere interest and determined intent to diminish the prevalence of ID Theft crimes. Chairman Kyl also showed great empathy for the trials and tribulations a victim of ID Theft endures and a sincere desire to make the system more "victim" friendly. On the last page of my Senate testimony, I included a list of 15 recommendations that I felt were important from my perspective as an ID Theft victim. One of my recommendations to the Subcommittee was to implement a uniform ID Theft victim reporting affidavit. As stated earlier, as victims of ID Theft we had been required to fill out dozens of different affidavits and follow dozens of different protocols to satisfy the merchants' requests for information and documentation as we tried to dispute fraudulent charges and restore our credit. I am pleased to say that through the intervention of Senator Kyl, the Subcommittee, and the FTC there is now a uniform ID Theft Affidavit. This ID Theft Affidavit will substantially diminish the amount of time

an ID Theft victim has to spend filling out forms and paperwork as they try to restore their credit and dispute fraudulent accounts.

My extensive efforts to try to obtain a federal investigation into our ID Theft case were unsuccessful. Senator Jon Kyl and James McDermond intervened, and that resulted in the United States Secret Service and Postal Inspection Service initiating a federal investigation. Richard Starmann, USSS; Christine Hoskins, USPIS; and Robert Himmelein, SSA/OIG all became involved in investigating our case.

Shortly after the federal authorities became involved in our case, I learned the fate of the Ford Expedition, the same Ford Expedition that had all of the glaringly obvious errors on the loan application. The criminals who had fraudulently purchased the Ford Expedition had torched the Ford Expedition and filed a fraudulent insurance claim in my husband's name. The criminals were now seeking to collect the insurance proceeds from this arson. As a result of this, we were now also dealing with the National Insurance Fraud Bureau. We were required to notify our own insurance company to put them on notice that the fraudulent insurance claim was filed by criminals, not by us. These criminals had collectively applied for $150,000.00 worth of new loans in our names, trashed our credit, filed a fraudulent insurance claim, and committed arson in my husband's name.

As victims of Identity Theft, our lives were turned upside down. We lived with a degree of fear that permeated every aspect of our lives. We not only placed the Fraud Alerts on our credit reports; we placed security protocols on our bank accounts that required photo ID and password (not mother's maiden name) for any transaction; canceled our credit cards; alerted our employers; notified the IRS; placed 7 year consumer statements on our credit reports and alerted our medical insurance company. Identity Theft had violated many areas of our lives.

Through the cooperation of our local police department, Chief Edward Matty wrote a letter on police letterhead stationary that stated we were the victims of financial crimes and Identity Theft. This was a notarized letter signed by Chief Matty. Identity Theft criminals were committing crimes using our names, and potentially having arrest warrants issued under our SSN's. I carry this letter with me at all times, as does my husband and both of our adult children. We all run the risk of being subject to mistaken arrest if we are pulled over for a traffic violation and arrest warrants appear under our SSN's numbers.

At the time I testified to the Senate Subcommittee, I had logged over 400 hours of time trying to clear our names and restore our good credit. I had accumulated hundreds of pages of ID Theft paperwork and documentation. Words are unable to adequately express the gamut of emotions that we have experienced as victims of ID Theft. The impact of being a victim of Identity Theft is all encompassing. It affects you physically, emotionally, psychologically, spiritually and financially. This has truly been a life altering experience.

Identity Theft has become a national epidemic. Banks and merchants are being defrauded out of billions of dollars each year by Identity Theft criminals. Innocent victims are having their credit ruined and financial reputations destroyed. We all pay the price through the higher cost of consumer goods, and higher interest rates on loans and credit cards. This epidemic must be stopped. The compromising of real identities is now the weakest link in the chain of financial transactions.

Once you become a victim of Identity Theft your life is forever changed. We still feel like we are "waiting for the other shoe to drop". We did not know how many more accounts might still be outstanding, we did not know if a collection specialist was calling when our phone rang and we did not know if our good names and financial reputations would ever be truly restored.

What we did know was that the impostor who had been arrested on November 18, 1999 by the Lansing Illinois detectives, the one who had been released on the signature bond in spite of an extensive criminal background and 17 aliases, appeared in court as the case progressed. This criminal was interviewed numerous times by the federal investigators and offered sentencing consideration in exchange for divulging accurate information. He declined to disclose any information, and was eventually sentenced to three years in the Illinois Department of Corrections. The time he actually served amounted to a little more than a year.

Our lives would never return to the "normal" status we had enjoyed prior to becoming ID Theft victims. The criminals receive a sentence of a specific duration, the ID Theft victim's sentence lasts for the rest of their life. There are frequent and often daily reminders of the trauma we endured as ID Theft victims. However, we thought the worst of the ID Theft nightmare was now behind us. That turned out to be wishful thinking on our part.

In the spring of 2001 we were in the process of trying to purchase a second home at the western end of Ohio, about 150 miles away from our primary residence. Both of our adult children are students in that vicinity, and purchasing a home there would substantially reduce the rent and dormitory expenses they were incurring. Our credit reports had been cleared of all of the derogatory accounts that had appeared as a result of our ID Theft victimization, and we proceeded with the intended purchase. As I stated earlier, I am a licensed Realtor, therefore, I am very familiar with the mortgage loan process. We wrote an offer to purchase a home, and I went to the KeyBank branch in that area to transfer the earnest money deposit from our savings account to our checking account. Please note that I had placed security protocols on all of our accounts as a result of our ID Theft victimization in 1999. Our local KeyBank branch employees had been honoring the protocols since I placed them on the accounts. Yet, when I transferred the money at an out of town KeyBank branch where I had never before done any transactions, I was not asked to present my photo ID or give my password. I informed the branch manager of the required protocols, and she reviewed our account information, which was displayed on the teller's screen. The manager scrolled through quite a few computer screens before the security protocol information appeared that stated our

accounts required photo ID and password. I found this to be not only absurd, but totally unacceptable. I insisted that the security protocols appear on each and every screen of our bank accounts, and the branch manager phoned our home branch of KeyBank to ensure that this was accomplished. The account screens were reviewed to verify that the tellers were prompted on every screen to require the security protocol.

After our offer to purchase was accepted, I started the mortgage application process. I chose a lender that I had done business with in our home community that had a branch office in the area in which we were purchasing the second home. I had forewarned the loan officer to expect to see Fraud Alerts and consumer statements on our credit reports and I told her we had been victims of ID Theft. I made the mortgage loan application in person, presented my driver's license, showed the loan officer my letter from Chief Matty and a copy of my Senate Subcommittee testimony. All appeared to be going well, until the loan officer pulled the copies of our credit reports. There was now a "derogatory account" appearing on my husband's credit report. Remember the fraudulent purchase of the Ford Expedition by the Illinois criminals in 1999? The one where there were multiple glaringly obvious errors on the fraudulent credit application. The same one that was torched and criminals filed the fraudulent insurance claim in my husband's name. The bank that financed the Ford Expedition, Firstar Bank, had posted a "derogatory account" on my husband's Experian credit report. This "derogatory account", which had never previously appeared on our credit reports, lowered my husband's FICO credit score by 118 points and we ran the risk and embarrassment of being denied the mortgage loan for the home we were legitimately trying to purchase. I was livid!

I now had to again battle with the credit reporting agency to have this "derogatory account" removed from this credit report. My previous and rather extensive efforts in having fraudulent accounts removed from our credit reports had been a very time consuming process. However, time was now of the essence in getting this "derogatory account" removed from the credit report. Our purchase agreement for buying the home contractually required that we obtain loan approval within 25 days or we would lose the house. I was frantic as I started making the calls to try to have this remedied.

I again contacted Kathleen Lund at the FTC to let her know about the "derogatory account". I also contacted Sen. Kyl's office, and Jim McDermond assisted us in trying to get the "derogatory account" removed. Experian did eventually remove the "derogatory account", but it required great effort on my part and Jim McDermond's part to get this accomplished. The real Ray and Maureen Mitchell were almost unable to legitimately obtain a mortgage loan, in spite of the extensive efforts I had expended cleaning up our credit. My friend, Cathy Teschke, summed it all up when she stated to me: "You know, Maureen, you should have had the criminals apply for the mortgage loan; they would have gotten it with no problem!" There may be more truth than any of us care to admit in Cathy's statement.

The mortgage loan was finally approved, and we again hoped our ID Theft nightmare was behind us. We learned that it wasn't as we attempted to purchase and

finance a refrigerator for the house we just bought. Best Buy had a 12 month same as cash promotional offer on appliances, and we applied for this promotional financing. We were denied the credit for the purchase of the refrigerator. As embarrassing as it was to be denied credit to purchase the refrigerator, it was gut wrenching to realize that our credit worthiness might never truly be restored. Criminals had no trouble obtaining credit in our names, but now we couldn't even finance a refrigerator!

Our next ID theft problem surfaced on October 30, 2001. I received a phone call at home from a woman who identified herself and said she was a KeyBank branch manager. She was calling to ask if we were having "trouble" with our bank accounts. I told her we were victims of ID Theft and had security protocols on our KeyBank accounts. She said she was placing a "security freeze" on our accounts, and I would be contacted by a KeyBank fraud investigator. I obtained the information I needed to reach her and to verify that she was a Keybank employee. I then contacted our local KeyBank branch, spoke to an employee I had known for years, gave her my password and asked her to check our accounts. There was indeed "trouble" with our bank accounts, and a security freeze had just been placed on our accounts. Four fraudulent withdrawals had been made from two of our Keybank savings accounts, and it was the attempt at a fifth fraudulent withdrawal that finally prompted KeyBank to contact me. The withdrawals were not made at our local KeyBank branch; they were made at three different Keybank branches in the greater Cleveland area. Criminals successfully made four fraudulent withdrawals, from two different savings accounts at three different KeyBank branches in spite of our security protocols requiring photo ID and password. I was stunned and furious! How the hell this could have happened was beyond my ability to comprehend. These fraudulent withdrawals collectively totaled $34,006.50. Criminals absconded thirty- four thousand six dollars and fifty cents from our bank accounts! And, as a result of the security freeze that was placed on our accounts, we had no access to our own money! We had banked with KeyBank for close to twenty years and were well known to the employees at our local branch, yet we had no access to our own money. Words will never adequately express the emotional turmoil we were experiencing as a result of our security protocol protected savings accounts being infiltrated by criminals.

The dates of the fraudulent withdrawals from our KeyBank accounts were two years after our initial ID Theft victimization. We knew the fraud alerts on our credit reports were good for two years, and I had conscientiously and intentionally renewed the fraud alerts well before the fraud alerts were set to expire. My intent in renewing the fraud alerts early was to try to stay one step ahead of the criminals. However, instead of criminals fraudulently applying for out-of-state loans in our names, they were now infiltrating our security protocol protected bank accounts in our home state, in essence in our own back yard. The criminals in Illinois who fraudulently obtained credit were impostors posing as my husband. Now there was a criminal impostor posing as me in Ohio. The resulting fear that now permeated the very essence of our being is indescribable.

I was again filing yet another police report, and also filing a KeyBank "Affidavit of Fact" report. Contact had been established with the KeyBank fraud investigator, Fred,

and an investigation into the events was initiated. Fred confirmed our accounts were frozen and told us that no activity would occur on the accounts. I had dozens of questions that I wanted answered immediately. One of the first things I wanted to know was how the hell criminals were able to withdraw the money with the security protocols in place. And I asked if the security protocols were even followed. Fred stated that the bank was "looking into it". I also wanted to know if the criminals had used our password. We needed to know immediately as to whether or not our password was compromised. Fred was unable to give us an answer. I also inquired if the same KeyBank teller was involved in each of the four fraudulent withdrawals. Fred said he would find out and let me know. I asked lots of questions, unfortunately, I did not receive many answers. My conversation with Fred, in my opinion, was not going very well. He was unable to answer my questions, and I wanted immediate answers. I also perceived a degree suspicion emanating from Fred that was directed at us. Fred seemed to be questioning our integrity, which I greatly resented. We are not criminals, we had not made nor had we authorized the withdrawals; we were previous ID Theft victims who had insisted on placing the security protocols on the accounts in the first place. The conversation went from bad to worse when Fred stated that after KeyBank investigated the circumstances of the fraudulent withdrawals "the money would probably be restored" to our accounts. I was irate to hear "probably restored". I stated to Fred, in no uncertain terms, that since KeyBank had allowed criminals to infiltrate our security protocol protected bank accounts not once, not twice, but four different times "there is no probably about it, our money will be restored, with interest!" I strongly suggested to Fred that he secure the bank surveillance tapes and pull our signature cards to prove to him that we were not the ones who made the withdrawals.

I asked Fred the date of the first fraudulent withdrawal; he told me it was done on Oct. 26, 2001. I then asked Fred for the date that KeyBank cut their Oct. statement; he said Oct. 25, 2001. I pointed out to Fred that the first fraudulent withdrawal was made the day after KeyBank cut their monthly statement. These dates were significant in my mind because the KeyBank statement that was due to arrive in my mailbox at any minute would not show the fraudulent withdrawal because it had been made right after the monthly statement was issued. Therefore, the criminals would have had a one month "head start" before the withdrawal would appear on my bank statement. I asked Fred if that did not indicate to him a "degree of sophistication" on the part of the criminals. Fred replied to me that it was "coincidence". I do not think it was "coincidence"; I think the criminals are smarter than many of the investigators.

We learned that three of the fraudulent withdrawals were in the amount of six thousand ($6,000.00) each, and the fourth fraudulent withdrawal was in the amount of sixteen thousand dollars ($16,000.00) The $6.50 appeared as a "charge" to our account posted on the same day that three out of the four fraudulent withdrawals had been made. And, in spite of the fact that there was thirty-four thousand six dollars and fifty cents ($34, 006.50) missing from our now frozen bank accounts, Fred was focusing on the six dollars and fifty cents ($6.50). Fred stated that the "six dollars and fifty cents" withdrawal from our accounts "must have been done" by us. I again firmly and emphatically told Fred we had not made any of the withdrawals. Fred then told me he

found it hard to believe that "a criminal would withdraw $6.50". I told Fred that I was not a fraud investigator; however, by now I felt that I had earned a PhD. from the school of ID Theft hard knocks and that I could think of two reasons for the $6.50 withdrawal. One reason was that criminals might have been testing the accessibility of the accounts between major withdrawals, and the other more likely reason was that the criminal took all or part of a withdrawal in the form of a bank check and the $6.50 was the chargeback to the account for the cost of the bank check. Turns out, I was right about the charge-back. When the criminal made the $16,000.00 withdrawal, she took half in cash and half in the form of a bank check. And, the bank check had been issued payable to Maureen Mitchell!

The fact that this bank check was made payable to Maureen Mitchell is very significant. This impostor now had in her possession an $8, 000.00 bank check issued in my name. Each time an impostor obtains an official piece of documentation in the name of the victim it gives the impostor additional "credibility" in assuming the identity of the victim. KeyBank not only gave our money to an impostor on four different occasions, KeyBank also gave the impostor a bank check in my name.

Additional problems arose for us as a result of our frozen bank accounts. All of our KeyBank accounts were frozen, not just the accounts the criminals had infiltrated. The criminals had not infiltrated our checking account, but we were now unable to write checks or access any of our KeyBank funds. We had bills that were due to be paid: mortgage payments, utility bills, credit card bills and college tuition to name a few. We asked how long the freeze would remain on our accounts, but no one from KeyBank could tell us when the accounts would be unfrozen. To complicate matters further, there were four checks that we had written just days before our accounts were frozen that had not cleared our checking account before the freeze was placed on our accounts.
I asked Fred what would happen to those checks; Fred told me the checks would be returned. I asked Fred if that meant the checks would come back "insufficient funds", Fred said the checks would be returned stamped "refer to maker". I requested that these four checks be allowed to clear our checking account, and offered to provide KeyBank with each check number, the amount the check had been written for, and the name of the entity to whom the check had been made payable. These checks had been written by us to our grocery store, our newspaper carrier, our church and my alumni association. Fred said he could not allow these checks to clear our account even though I could provide all of the information contained on these checks. As a result of the return of these checks to the payee stamped "refer to maker", we received a letter in the mail from a collection agency. This letter stated that we had been turned over to collections for the check that we had written to our grocery store, as it had not been honored by KeyBank. The letter stated that there was a $30.00 collection charge that was added to the amount the check had originally been written for, and went on to say this collection agency "has been designated to collect payment and will record your checking account number in our check verification database, which can affect your check cashing ability at many retail establishments." As a result of KeyBank's failure to honor this check we were placed on a "bad check list".

I showed our local KeyBank branch manage the letter from the collection agency, and efforts were made to get our names and checking account number out of the collection agency's database and to waive the $30.00 collection penalty. Those efforts were unsuccessful until I contacted the owner of the grocery store, explained the events that lead up to the frozen accounts, which resulted in the check not being honored and returned "refer to maker". The grocery store owner then contacted the collection agency and the situation was eventually resolved.

My contacts with Fred continued, and I received additional information from contacts I initiated with the KeyBank branches where the fraudulent withdrawals had been made. I asked for a physical description of my impostor. I was told she was "a 5'5" brown eyed African American with auburn hair pulled back in a French twist" and that she was "calm and svelte". I am a 5'3" Caucasian American with green eyes who by this time was far from calm and certainly not svelte. KeyBank's investigation continued, and our accounts remained frozen. I was still unable to access any of the money in our KeyBank accounts to pay our bills. And we were living with each day with a great deal of fear and uncertainty. The criminals had invaded the most private area of our lives, our personal finances and this second round of Identity Theft crimes had been committed in our home state. I was born, raised and educated in New York City and I am usually not a woman who gives in to fear, however, the trauma of being a two-time ID Theft victim was exacting a huge toll. Our entire family was affected by the stress. It's a horrible feeling to know that criminals are privy to your most private information. Some of our friends equated the trauma we were enduring as "financial rape". That's as close as any of us could come in trying to put into words what we were feeling. We were doing our best to cope with the fear and the rage. I was absolutely incensed that the security protocols on our KeyBank accounts failed to work, that our accounts were frozen, that we couldn't pay our bills and that we were placed on a bad check list with a collection agency.

On Sunday, Nov. 4, 2001, we received a phone call at home that added to our trauma. The caller identified herself as Joanne, and said she was calling from First North American National Bank in Georgia. Joanne wanted to know if I had just applied for a $5,000.00 line of credit at Circuit City. I quickly told Joanne that we were ID Theft victims, and had not applied for any credit. Joanne said she was calling because she saw the Fraud Alert on my credit report as she was trying to process a credit application that had just been made in my name. I asked Joanne to tell me the location of the Circuit City store where the application had been made. Joanne said she only had a location number for the store, not an actual store address. I told Joanne that I needed the address immediately, as we had just experienced local criminals infiltrating our bank accounts. Joanne promised to locate the store address and call me back. It was only a matter of minutes before Joanne called back, and told me the Circuit City store was located in North Randall Ohio. North Randall lies on the outskirts of Cleveland. Joanne put me on a conference call to the Circuit City store, and we spoke to the store manager. I told the store manager that if "Maureen Mitchell" was in the store applying for credit to pretend that the bank was working out a credit glitch, and it would take a few minutes before they could extend credit to her. I then told him that she was an impostor, I was the real

Maureen Mitchell and I wanted him to call the police immediately. He placed us on hold, walked to another phone and whispered to us that the impostor had been standing right next to him as we were speaking. He told us that he police were called, and that the impostor was still in the store. Within a matter of minutes the North Randall police arrived and arrested the impostor. I could hardly find the words to thank Joanne and the store manager. It was such a relief to know that an arrest had been made. One of the arresting officers picked up the conference call and told me they were transporting the suspect to the North Randall police station, gave me the station's phone number and instructed me to call there in 20 minutes. While waiting to place that call, I had the opportunity to continue to speak to Joanne. Joanne told me that she knew from the Fraud Alert and consumer statement on my credit report that I had been a victim of ID Theft. Joanne said she had spoken to the impostor on the phone as the impostor belligerently tried to assert that she was the real Maureen Mitchell. Joanne knew it was an impostor when she asked the impostor questions related to my credit report that only I would know the answer to. Joanne also told me that when the impostor filled out the credit application she had tried to change my address. The impostor even had the nerve to request that Joanne send her a copy of "her" credit report at the "her" address.

I called the North Randall police department and was told that the suspect they arrested possessed what appeared to be an Ohio BMV issued photo identification card. This card was issued in my name, had my home address, and my driver's license number. This card also had the impostor's picture! I asked the officer if it was a real BMV identification card, or had it been manufactured in some criminal's basement. I was told the card appeared to be an authentic BMV issue. I asked for a physical description of this suspect, and it was very similar to the description I had been given of the impostor who infiltrated our KeyBank accounts. I also asked the officer how the BMV could have issued a photo identification card that displayed my name, my address, and my driver's license number to a woman who looked nothing like me. My photo had been in the Ohio BMV's data base since I got my Ohio driver's license in 1978. The officer told me I would have to ask the BMV those questions. I told the officer of our ID Theft victimization, and that an impostor had recently made fraudulent withdrawals from our KeyBank accounts. I was speaking with this officer on a Sunday night and was told I could call the station on Monday morning and the officers would have more information.

On Monday morning I placed numerous phone calls to the Ohio BMV to find out how an impostor could have obtained an identification card from the BMV that displayed my personal information but the impostor's picture. I eventually reached an investigative officer of the BMV and was appalled to learn that not only had the BMV issued the photo identification card to the impostor, the BMV also suspended my driver's license when the impostor obtained the photo identification card. I couldn't believe what I was hearing; my driver's license had been suspended! I asked the investigator how that was possible and he explained that in Ohio it is illegal to concurrently have an Ohio driver's license and an Ohio BMV issued photo identification card. When the impostor obtained the photo identification card, she signed away my driving privileges in the state of Ohio for life, and my license was suspended. I then asked why I wasn't notified by the BMV that my license was suspended, and I was told they would eventually send me a letter. I

inquired as to the date my license suspension occurred, and was told it was Oct. 25, 2001. That was the day before the impostor made the first fraudulent withdrawal from our KeyBank accounts. I was also told that I would have to meet with a BMV fraud investigator at a Deputy Registrar's office of my choosing. I asked if they would like me to "flap my wings to get there"; they had suspended my driver's license. I was also instructed to bring plenty of proof of identification because I would have to prove I was the real Maureen Mitchell. I asked if they would like to use my suspended driver's license as valid proof! I was also told that as a "courtesy" the State of Ohio would waive the requirements for the written test, the road test and the re-licensing fee.

I was absolutely heartsick to realize our bank accounts were frozen, our names were on a bad check list and my driver's license was suspended. I hold three licenses in the State of Ohio; my driver's license; my real estate license; and my R.N. license. After learning my driver's license was suspended, I was extremely fearful that my professional licenses might also be suspended as a result of the actions of my impostor.

I met with the BMV fraud investigator and brought my entire briefcase full of Identity Theft paperwork. I showed him the notarized letter from Chief Matty and gave him a copy of my Senate Subcommitee testimony. He then went through the BMV required protocol to issue me a new driver's license. He faxed the necessary forms to Columbus to obtain a Columbus issued driver's license number that was supposed to be "coded" to let law enforcement know that it was a re-issued license to an ID Theft victim. I sat for the driver's license picture, and waited for the license to be processed. I was astounded when I read the physical description that was printed on my new license. My new license said I was 5'5" with brown eyes! The criminal's information overrode my information in the BMV database. We had to start the whole process over again, and the Deputy Registrar had to manually type in my correct physical description.

When KeyBank was finally ready to unfreeze our accounts, we arranged to close our accounts. We still do not know if the KeyBank tellers who gave my impostor our money were complicit or inept. The facts, as we saw them, were that KeyBank could not keep our money safe; therefore, KeyBank would no longer have our money. KeyBank unfroze our accounts during non-business hours and cut us cashier's check to close the accounts.

I contacted Kathleen Lund at the FTC to update her on the arrest of my impostor. I also informed Fred, the KeyBank fraud investigator, of the arrest. We were eventually told that the impostor who had been apprehended at the Circuit City store confessed to the fraudulent KeyBank withdrawals. My impostor also had a criminal history, and is currently incarcerated on probation violations. She was indicted by the Cuyahoga County grand jury on Identity Theft charges. I registered with the Cuyahoga County Witness/Victim Service Center, and will be kept informed of the judicial process as it progresses. Our case is currently pending

As victims of Identity Theft we will always carry the emotional, psychological, and financial scars. To this day we still do not know how the criminals obtained our personal information. Our "point of compromise" has yet to be determined.

We hope and pray that our Identity Theft nightmare is finally over.

The tragic and horrific events of September 11, 2001 serve as a horrible reminder of the extent and the reach of the crime of Identity Theft. Congressional testimony delivered in November 2001 revealed that the 19 hijackers had multiple aliases and several assumed identities. Some of the hijackers had more than one SSN. James Huse, the Inspector General of the SSA testified: "We know now, without question, that this illegal activity not only facilitates financial crimes but provides capability for organized criminals to sustain themselves while engaged in acts of terrorism." Identity Theft is not only wreaking havoc with the lives of its victims, Identity Theft is funding terrorism.

The epidemic of Identity Theft must be stopped. ID Theft crimes have cost our country billions of dollars in recent years. On September 11, 2001 Identity Theft facilitated terrorism and cost our country thousands of lives.

Thank you for the opportunity to submit this testimony.

Respectfully submitted,

Maureen V. Mitchell

STATEMENT OF JOSHUA L. PEIREZ
SENIOR VICE PRESIDENT AND ASSISTANT GENERAL COUNSEL
MASTERCARD INTERNATIONAL INCORPORATED

BEFORE THE
HOUSE COMMITTEE ON FINANCIAL SERVICES
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

"FIGHTING IDENTITY THEFT – THE ROLE OF FCRA"

JUNE 24, 2003

Good morning, Chairman Bachus, Congressman Sanders, and Members of the Subcommittee. My name is Joshua Peirez and I am Senior Vice President and Assistant General Counsel at MasterCard International in Purchase, New York. MasterCard is a global organization comprised of financial institutions throughout the world that are licensed to use the MasterCard service marks in connection with a variety of payment systems. For example, these member financial institutions issue payment cards to consumers and contract with merchants to accept such cards. MasterCard provides the networks through which the member financial institutions interact to complete payment transactions—MasterCard itself does not issue payment cards, nor does it contract with merchants to accept those cards. I thank the Subcommittee for having a hearing on this critically important issue and for giving me the opportunity to appear before you to provide information on combating identity theft.

MasterCard takes its obligations to protect MasterCard cardholders against identity theft and other forms of fraud very seriously. In fact, this issue is a top priority for MasterCard, and we have a team of experts, including many former law enforcement personnel, devoted to combating all types of fraud. We are proud of our strong record of working closely with federal, state, and local law enforcement agencies to apprehend these criminals. Included among the federal law enforcement agencies with which we work closely are the Federal Bureau of Investigation, the U.S. Secret Service, the Federal Trade Commission, the U.S. Postal Inspection Service, and others at both the federal and local level. MasterCard also fields calls from local law enforcement virtually every day. MasterCard believes its success in fighting fraud is perhaps best demonstrated by noting that our fraud rates have continuously declined over time and are at historically low levels as a percentage of transactions.

MASTERCARD CONSUMER PROTECTION AND FRAUD PREVENTION

MasterCard recognizes that identity theft and other fraudulent schemes evolve constantly, and we devote substantial resources to staying one step ahead of the criminals. We continually develop new ways to protect MasterCard cardholders and to make fraud more difficult. The following is a brief overview of just some of the efforts MasterCard has made in this area.

Issuers Clearinghouse Service

The first step in combating identity theft and other similar types of fraud is to develop techniques to prevent the crime from occurring in the first place. In our experience, accurate, reliable information is the most critical element in any identity theft prevention program. In an effort to enhance the ability of our member financial institutions to combat identity theft and other types of fraud, we require our members in the U.S. to participate in the Issuers Clearinghouse Service ("ICS"), a system built using data provided by issuers regarding, among other things, the fraudulent use of consumer data. More specifically, MasterCard's U.S. members provide ICS with data regarding customer addresses, phone numbers, and social security numbers that have been associated with fraudulent activity. MasterCard members are also required to access ICS in connection with each application to open a MasterCard account. The ICS database helps financial institutions to detect suspicious activity and prevent identity theft and other fraud before it occurs. For example, the centralized ICS database allows MasterCard members to notice whether a particular social security number was used to open a number of accounts using different addresses. Such activity may indicate that the social security number is being used for identity theft or some other fraudulent scheme. In this way, ICS provides our member financial institutions a specialized fraud prevention tool that acts as an enhancement to their other fraud prevention efforts, including those that rely on accurate, reliable consumer reports they receive under the federal Fair Credit Reporting Act ("FCRA") as discussed in greater detail below.

Payment Card Security Features

Another key part of the MasterCard fraud prevention efforts is the security features built into the payment card itself. For example, MasterCard has worked hard to make it difficult for a criminal to make use of a card number in transactions where the card is not present, such as in telephone, mail, or Internet transactions. One tool to ensure that the person presenting the number is actually the cardholder is the added security features on the card itself. MasterCard cards have the full account number printed on the card with an additional three digits on the back of the card. Many phone, mail, and Internet merchants now request these additional three digits as part of the consumer's payment transaction. In this regard, these three digits act similar to a PIN for the card and can be used to ensure that

the person presenting the card number actually has possession of the card—not just the account number.

Address Verification

Another tool to fight fraud is MasterCard's Address Verification Service ("AVS"). A criminal who obtains access to a MasterCard account number is unlikely to know both the name and the billing address of the individual who holds the account. MasterCard has developed its AVS to take advantage of this fact and prevent the criminal from using the account number. Merchants accepting a MasterCard account number by phone, mail, or Internet are increasingly using AVS as a resource and are asking for the consumer's billing address. At the time of payment, the merchant submits the billing address into the MasterCard system to verify with the card issuer that the name and billing address match the account number provided. If AVS indicates that the billing address and the account number do not match, the merchant can take additional steps to verify that the person presenting the number is the legitimate cardholder, or the merchant may simply decline the transaction.

MasterCard SecureCode

MasterCard has developed a relatively new service that allows issuers to provide added security to their cardholders when the cardholders shop on-line. A cardholder registers his or her MasterCard card with the issuer and creates a private SecureCode. Each time the cardholder makes a purchase at a participating merchant, a box will automatically pop up asking the consumer for the SecureCode—similar to the way an ATM will ask for a PIN when withdrawing money. When the cardholder correctly enters the SecureCode during an on-line purchase at a participating merchant, the cardholder confirms that he or she is the authorized cardholder. If the correct SecureCode is not entered, the purchase will not go through.

"SAFE" (System to Avoid Fraud Effectively)

MasterCard's System to Avoid Fraud Effectively ("SAFE") program is a multi-purpose tool to thwart fraud. The SAFE program is built, in part, through the use of data provided by MasterCard issuers regarding fraud-related transaction information. For example, data regarding fraudulent merchants, transactions, and other patterns of activity is incorporated in the SAFE program for use by MasterCard and its members. The SAFE program allows MasterCard to identify fraud at merchant locations and allows us to better focus our global merchant auditing programs. The SAFE program also allows us to identify potentially fraudulent actors relatively early in the process, before the problem escalates.

Site Data Protection Service

MasterCard's Site Data Protection Service ("SDP") is a multi-tiered, comprehensive set of global e-commerce/financial security services designed to help protect the web sites of its members and their on-line merchants from hack and attack. MasterCard designed SDP to be a cost-effective diagnostic tool for members and merchants to allow them to understand any systems vulnerabilities they may have. Furthermore, SDP also recommends actions that can be taken to reduce the potential systems vulnerabilities.

MasterCard's Zero Liability Protection

Recognizing that no system of protections will ever be perfect in preventing identity theft and other fraud, MasterCard has taken an important step to ensure that MasterCard cardholders are not held financially responsible when they are victimized by fraud involving U.S.-issued MasterCard accounts. We believe that our cardholder protections are the strongest available and among the most important consumer benefits a cardholder has, as these benefits provide consumers with the security and comfort necessary to make MasterCard "the best way to pay for everything that matters." A key element of our cardholder protections is our voluntary "Zero Liability" rule with respect to the unauthorized use of U.S.-issued MasterCard consumer cards. It is important to note that MasterCard's protection with respect to Zero Liability is superior to that required by law. The Truth in Lending Act imposes a $50 liability limit for the unauthorized use of a credit card. Under the Electronic Fund Transfer Act, the cardholder's liability for the unauthorized use of a debit card can be higher. MasterCard, however, provides all U.S. MasterCard consumer cardholders with even more protection. Under our rules, a cardholder victimized by unauthorized use generally will not be liable for any losses at all. This means that it is the financial institutions, and not the cardholders, that bear the financial loss when a MasterCard cardholder is victimized by identity theft or other fraud. This has greatly enhanced consumer confidence, including with respect to shopping on-line. A MasterCard cardholder can shop anywhere in the real or virtual world with the confidence that he or she will have no liability in the event that his or her account number is used without authorization.

THE IMPORTANT ROLE OF THE FCRA IN PREVENTING IDENTITY THEFT

As noted above, one of the most important tools in combating identity theft is the availability of accurate, reliable information about consumers. The role of providing this data has primarily been taken on by our nation's three major credit bureaus—Equifax, Experian, and TransUnion. These credit bureaus gather information from thousands of sources commonly referred to as "furnishers," and compile the information into individualized reports about consumers. These consumer reports contain the most accurate and reliable data available about the identities of consumers and other characteristics which are essential in combating identity theft. For example, when a bank receives an application from a consumer through the mail, the consumer report obtained from a credit bureau can be the single most important piece of information to the bank in determining whether the

individual who submitted the application is an identity thief or not. Indeed, the status of credit bureau data as useful and reliable information for identification purposes has been recognized and embodied in this nation's anti-terrorism efforts. For example, the regulation promulgated by the U.S. Treasury Department to implement Section 326 of the USA PATRIOT Act relies heavily on the use of consumer reports in properly identifying individuals who become customers of financial institutions.

The reliability of consumer report information as an identity theft prevention tool is due in great measure to the national uniform standards for credit reporting established under the FCRA. The following are some key examples of how national uniformity has ensured the quality of our credit reporting databases and has helped to combat identity theft.

Furnisher Obligations

MasterCard issuers are among the most significant suppliers of information to credit bureaus. These financial institutions report information about their accountholders regularly to the three major credit bureaus. The information generally includes the fact that an account has been established, the line of credit and current balance on the account, when the account was established, and whether the consumer has been delinquent on any payments.

Furnishers have certain obligations under the FCRA, and these obligations are the same across the country as a result of the uniform standards established by the FCRA. For example, if a furnisher determines that information it has reported to a credit bureau is not complete or accurate, the furnisher must promptly notify the bureau and provide any information necessary to make the information complete and accurate. In addition, if a consumer disputes the accuracy of information with a furnisher, the furnisher may not provide the information to the credit bureau without a notice that the accuracy is disputed. Furnishers also must reinvestigate alleged errors about information they provide to credit bureaus.

These obligations were established in 1996 in an effort to address concerns about the accuracy of information received by credit bureaus. The furnisher obligations were carefully crafted to balance between the need for furnishers to provide accurate information to credit bureaus and recognition of the fact that furnishing information to credit bureaus is completely voluntary. In particular, Congress recognized that imposing unreasonable liability or risk of litigation on furnishers could have a chilling effect on the flow of the information that is the lifeblood of the credit reporting system. As part of the delicate balance struck on this issue, and in recognition of the need for uniform information available nationwide, the FCRA precludes the states from imposing different standards.

It is important that this delicate balance be preserved. If a state were free to impose stricter liability standards on furnishers, many furnishers would be forced to re-evaluate the practice of furnishing information to credit bureaus with respect to consumers in that state. Indeed, many furnishers may have no choice but to stop furnishing information on consumers in that state rather than face the cost of litigation.

This would significantly reduce the reliability of credit bureau data. For example, card issuers and other similar financial institutions frequently have the most reliable information about a consumer's current address, change of name (*e.g.* as a result of a marriage or divorce), and other up-to-date identifying information. Stricter liability standards or more severe furnisher burdens imposed at the state level could very well curtail the availability of this information to credit bureaus and, consequently, to banks and other financial institutions that currently use it as an important identity theft prevention tool.

Contents of Consumer Reports

The contents of a consumer report are also largely standardized as a result of the national uniformity provisions of the FCRA. The FCRA establishes the time frames during which information becomes "obsolete" and can no longer be included in a consumer report. Generally, adverse items of information that are older than seven years cannot be reported in a consumer report (although the time frame expands to ten years for bankruptcy information). The FCRA preempts state laws with respect to any subject matter relating to information contained in consumer reports. This means that, as a general matter, someone's consumer report will look the same, regardless of the state in which they live. This also means that the identification information on the consumer report will be available regardless of where the consumer lives. A single standard with respect to the contents of consumer reports is critically important to ensure that the ability to properly identify customers, and therefore to provide financial products and services to them, is uniform across the country. In this regard, American consumers are extremely mobile, with millions moving from state to state in any given year. Financial institutions seeking to provide consumers with financial products or services across the country must be able to rely on a uniform standard for credit reports.

Prescreening

The FCRA governs the important underwriting and marketing tool known as "prescreening." Prescreening is a process under which a creditor may provide firm offers of credit to consumers who meet certain established underwriting criteria. Firm offers of credit often take the form of the "preapproved" offers that people receive in the mail. If an individual responds by requesting the credit, the creditor must honor the offer so long as the individual continues to meet the criteria for the offer. Each prescreened mailing also must include instructions as to how the consumer can "opt out" of receiving prescreened offers in the future. Under the FCRA, a consumer can opt out of future prescreening from the three main credit bureaus simply by calling a single toll-free number.

Prescreening is a powerful tool in combating identity theft and other fraud. In this regard, the incidence of all fraud including identity theft is dramatically lower for credit card accounts when those accounts are obtained through prescreening rather than through other channels. Thanks to the national uniformity established under the FCRA, the benefits of prescreening as a fraud prevention tool are available across the country. It is critically important that the FCRA's national uniformity regarding prescreening be preserved.

Affiliate Sharing Provisions

The FCRA also regulates the sharing of information among affiliated entities. In this regard, the FCRA provides that information may be shared among affiliates and gives the consumer the right to opt out of the sharing of consumer report information. Affiliate sharing programs are increasingly used to control identity theft and other risks. For example, a card issuer's ability to thwart an identity thief may be enhanced significantly when the issuer can obtain information from its affiliated mortgage lender regarding a mortgage loan it has extended to the real individual whose name is being used on the identity thief's application. The FCRA currently establishes national uniform standards for affiliate sharing. The availability of affiliate sharing as an identity theft prevention tool would be significantly undermined if states were free to impose their own restrictions on affiliate sharing activities.

CONCLUSION

MasterCard and its members take our obligations to protect MasterCard cardholders against identity theft seriously. At MasterCard we have a team of experts devoted to designing and implementing new and better ways to protect MasterCard cardholders from fraud, including identity theft. These initiatives complement our members' activities to fight fraud and prevent identity theft. However, an important component of our collective efforts to protect consumers is the FCRA. As I have discussed, a critical tool in the fight against identity theft is the availability of accurate, reliable information about consumers. The availability of this flow of information is protected under the framework of a single uniform national standard established by the FCRA. I urge you to help ensure this information remains available by making the national uniformity under the FCRA permanent.

Thank you again for allowing me to appear before you today. I am happy to answer any questions you may have.

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

TESTIMONY

Statement of

Chief Mary Ann Viverette
Third Vice President

Of the
International Association of Chiefs of Police

Regarding
Fighting Identity Theft

Before the
Subcommittee on Financial Institutions and
Consumer Credit
Committee on Financial Services
U.S. House of Representatives
June 24, 2003

515 N. WASHINGTON STREET
ALEXANDRIA, VA 22314
703-836-6767
WWW.THEIACP.ORG

Good Morning, Chairman Bachus, Representative Sanders and Members of the Subcommittee.

I am pleased to be here this morning on behalf of the International Association of Chiefs of Police (IACP). As you may know, the IACP is the world's oldest and largest organization of law enforcement executives, founded in 1894, and with a current membership exceeding 19,000. Our mission, throughout the history of our association, has been to address urgent law enforcement issues and to develop policies, programs, training and technical assistance to help solve those issues. And as I appear before you today, the issue of identity theft is one of great and growing concern to the law enforcement community. In a relatively short period of time identity theft has transformed from a relatively unnoticed crime to a major problem in the United States and around the world.

Growth of Identity Theft

As you know, identity theft is the wrongful use of another's personal information, such as credit card numbers, Social Security number, and driver's license number to commit fraud or another form of deception. This is usually done for monetary gain, although there may be other motives.

The target of identity theft is information that will enable the thief to assume another's identity for a criminal purpose. In the last few years, personal information has become one of the commodities most sought after by criminals in this country and elsewhere. Because it is usually part of a larger criminal enterprise, the theft of personal information is one of the most serious of all crimes.

Although identity theft is in itself a criminal act under both federal and most state laws, the theft is almost always a stepping-stone to the commission of other crimes. Typical crimes associated with identity theft include credit card fraud, bank fraud, computer fraud, Internet fraud, fraudulent obtaining of loans, and other schemes designed to enable the perpetrator to profit from the original theft.

Furthermore, funds obtained illegally as a result of the identity theft and its resultant frauds may be used to finance other types of criminal enterprises, including drug trafficking and other major forms of criminal activity.

The escalation of identity theft in the United States is due in large part to the technology revolution that has brought the country into the so-called Information Age. The vastly expanded use of computers to store personal data and the growing use of the Internet have provided criminals with new incentives and new means to steal and misuse personal information. As the use of technology to store and transmit information increases, so too will identity theft. Consequently, identity theft will likely become an even greater problem in the future.

Impact of Identity Theft

The ability to accurately define the financial losses of the vast number of crimes committed by means of identity theft is not possible at this time. Many identity theft crimes are not reported to police, and there is no single source of information on this issue. It is fair to say, however, that the cumulative financial losses from identity theft and the various crimes that feed from it are staggering.

However, perhaps even more tragic than the monetary loss is the personal cost of identity theft. Because identity theft by definition involves the fraudulent obtaining of funds in the name of someone else, the victim of identity theft may sustain not only great financial loss, but also severe damage to credit standing, personal reputation, and other vital aspects of the victim's personal life. For example, the victim may suffer garnishments, attachments, civil lawsuits, and other traumatic consequences stemming from the identity theft. In some cases the victim may be forced into bankruptcy, further damaging his or her reputation and credit. In other instances, the victim may become subject to criminal prosecution because of crimes committed by the perpetrator of the identity theft in the victim's name.

Even if the victim ultimately clears his or her credit records and avoids other personal and financial consequences of identity theft, the physical and mental toll on the victim can be significant. Typically, a victim of identity theft will spend months or years trying to clear his or her credit records. Many hours of difficult and stressful effort are often necessary, because the merchants and institutions that have been defrauded in the victim's name are not easily persuaded that the victim is innocent of any wrongdoing. The frustration and distress engendered by this heavy burden often take a significant toll on the mental well being and physical health of the victim. And, worst of all perhaps, the victim's efforts to clear him or herself may be unsuccessful, leaving the victim under a cloud for the rest of his or her life.

Types of ID Theft and ID Theft Operations

As has been noted, the key target of identity theft perpetrators is personal and confidential information of individuals. There are so many methods by which identity thieves may acquire personal information that it is impossible to catalog them all here. However, the following methods are commonly used:

- Stealing wallets and purses containing personal identification, credit cards, and bank cards.
- Stealing mail, including mail containing bank and credit card statements, preapproved credit card offers, telephone calling cards, and tax information.
- Completion of a false change-of-address form to divert the victim's mail to another location.
- Searching trash for personal data found on such discarded documents such as preapproved credit card applications or credit card slips discarded by the victim.
- Obtaining credit reports, often by posing as a landlord, employer, or other person or entity that might have a legitimate need for, and right to, credit information.
- Obtaining personal information at the workplace or through employers of the victim.

- Discovering personal information during physical entries into the victim's home. Such entries may be unlawful, as in burglary, or initially lawful, as when friends, service personnel, or others are invited to enter the home.
- Obtaining personal information from the Internet. This may be information stolen by hackers or freely provided by the victim in the course of making purchases or other contacts.
- Purchasing information from inside sources such as store employees, who may for a price provide identity thieves with information taken from applications for goods, services, or credit. At least one instance has been reported of an employee of a credit bureau collaborating with identity thieves to provide personal information from credit bureau records.
- *Pretexting*, in which a thief telephones the victim or contacts the victim via Internet and requests that the victim provide personal information
- *Shoulder surfing*, a practice whereby the thief positions himself or herself near a victim in order to obtain personal information by overhearing the victim or seeing the victim's actions. For example, the thief may stand near a pay telephone in a public place and listen as the victim gives credit card number information or other personal information in the course of making a call. Similarly, thieves may loiter near an automated-teller machine (ATM) and visually observe the victim keying in password numbers on the machine.
- "Skimming," which is the electronic lifting of the data encoded on a valid credit or ATM card and transferring that data to a counterfeit card. There are many variations of this practice. For example, an identity thief may recruit an employee of a retail store, restaurant, or other retail establishment. The employee is provided with a hand-held electronic device that can read data from a person's credit card when the consumer presents it to the employee. The collusive employee then surreptitiously "swipes" the credit card through the hand-held "reading" device, which records the electronic data from the card. The employee then returns the device to the thief and the thief extracts the recorded data from the device.

- Identity thieves may also purchase personal information about potential victims from persons or entities that routinely collect such information. In some instances these entities may be legitimate, but in many cases they are criminal enterprises formed for the specific purpose of selling information to thieves.

How Stolen Information is Used

There are literally hundreds of ways in which identity thieves may use the information they have stolen. The following are just a few examples:

- Once they have a victim's credit card number, thieves may call the victim's credit card issuer and, pretending to be the victim, asks that the mailing address on the account be changed. The thieves then run up high charges on the credit card, and because credit card statements are no longer being sent to the victim's real address, the victim might be unaware of what is happening for weeks or even months.
- These same thieves who have obtained a victim's credit card information may also request that the credit card company send them credit card "checks," which are written for cash just as are bank checks. Again, the charges are unknown to the victim because the credit card statements are no longer coming to the victim's address.
- Having obtained personal information such as name, date of birth, Social Security number, and so on, the thieves open new credit card accounts in the victim's name and run up charges until the victim becomes aware of the fraud. Similarly, credit accounts may be opened at stores using the victim's identity.
- The thieves open bank accounts in the victim's name and write bad checks on the account.
- The thieves obtain loans, such as real estate, auto, or personal loans, using the victim's identity.
- The thieves counterfeit checks or debit cards, and drain the victim's bank accounts of funds.

- The thieves establish services such as utility, telephone, or cell phone service in the victim's name.
- The thieves make long distance calls using stolen credit card numbers.
- The thieves may obtain other goods and privileges by using the victim's identity and information, either in person or by telephone or via the Internet.

These are only a few of the numerous schemes that an identity thief may use to obtain money, goods, or services at the expense of the unwitting victim.

Perpetrators

Identity theft is not perpetrated only by so-called white-collar thieves. It is committed by criminals of all types. A recent report indicates that during the period November 1999 to March 2001, about 12 percent of all suspected perpetrators reported to the Federal Trade Commission had a personal relationship of some sort with the victim. However, the remaining 88 percent of suspects had no relationship to the victim of the theft. Thus, while the thief may be a family member, a coworker, a friend, or someone else personally known to the victim, in the vast majority of instances the perpetrators are unknown to the victim.

In most cases the thieves are geographically located far from the victim's place of work or residence. These perpetrators may be solo operators, but more often are members of a larger criminal organization. Such organizations may be local, regional, national, or international in scope. They may be composed of specific ethnic or national groups, or may be simply a collection of criminals of various backgrounds cooperating to obtain illegal profits at the expense of the innocent victims.

Law Enforcement Response

In earlier years, the involvement of local police departments in identity theft cases was typically minimal. In fact, many local police departments refused to take complaints about identity theft because the crime was not well understood. This was caused by several factors, including the lack of state laws making identity theft a crime, the fact that most identity theft operations are multi-jurisdictional enterprises, with perpetrator and

victim usually widely geographically separated, and the general lack of police expertise in investigating the crime of identity theft.

Fortunately, this situation is now rapidly being remedied. The passage of numerous federal and state statutes has given federal, state, tribal and local law enforcement agencies the authority to investigate and prosecute identity theft crimes, and departments everywhere are becoming more aware of the significance of identity theft and the availability of the means to combat it.

However, since identity theft and its resultant crimes often involve a wide variety of offenses and means of committing those offenses, effectively combating identify theft will require not only the dedication of significant resources but also greater collaboration and cooperation between federal, state, tribal and local law enforcement agencies. This information sharing among agencies is essential as it may not only lead to a successful prosecution of the case in one jurisdiction but concurrent investigation in other areas of the country. I am pleased to say that in recent years, federal, state, tribal and local law enforcement agencies have made significant strides in this area and are increasing our capability to investigate, track, apprehend and prosecute these criminals.

Nevertheless, the law enforcement community cannot effectively combat identity theft by itself. Citizens need to take proactive steps to protect their personal information. Businesses must act to establish safeguards that will ensure that the personal information of their patrons is not exposed. Policy-makers at all levels of government need to review current statutes to ensure that protection of personal information is a priority and develop legislation that will strengthen the penalties for identity theft.

Only by acting to establish greater protections of personal information and by aggressively tracking down and punishing those who commit identity theft can we hope to turn the tide in this battle.

This concludes my statement. I will be glad to answer any questions you may have.

Information Sharing Facts

MBNA Corporation

U.S. Deposit, Credit Card, Consumer Finance, and Credit Protection Products for Consumers

Information MBNA Collects to deliver top quality service you expect:	• Consumer identification information • Transaction and repayment information • Credit eligibility information
Information Shared within MBNA and with its partners to offer special products and services, exclusive discounts, and other promotions:	• Consumer identification information • Transaction and repayment information • Credit eligibility information
Information sharing choices available to you:	• Continue receiving information on special products and offers • Prohibit sharing of credit eligibility information within MBNA • Prohibit sharing of all information with other MBNA partners

To express your information sharing preferences:
You may prohibit either or both types of information sharing by calling MBNA's toll-free automated response line at 1-800-XXX-XXXX. We will ask you to verify your identity and the specific accounts to which your choices apply. Please have your account, membership, or reference numbers (and for deposit accounts, your SSN or TIN) available when you call.

To obtain the complete information sharing notice:
Federal Law requires us to provide this short-form privacy notice on an annual basis and provides exceptions allowing information sharing notwithstanding your privacy preferences. You may have other privacy protection under state law. If you would like to receive a copy of MBNA's complete privacy notice, please call toll-free 1-800-XXX-XXXX.

MBNA

Privacy Policy Highlights

DATED: MARCH 2003

This notice describes the privacy policy of MBNA Corporation and all its affiliates, including:
- MBNA America Bank, N.A.
- MBNA America (Delaware), N.A.
- MBNA Technology, Inc.
- MBNA Marketing Systems, Inc.
- MBNA Insurance Agency, Inc.

At MBNA, we are committed to providing you with the finest financial products and services backed by consistently top-quality service. And while information about you is fundamental to our ability to do this, we fully recognize the importance of keeping personal and account information secure. Here is a brief overview of MBNA's privacy policy.

- We collect basic identification information, such as name and address.
- We collect basic transaction information, such as purchases and payments.
- We collect credit eligibility information, such as credit reports.

- We share information within MBNA companies to offer you new products and services.
- We share information with our partners so they can offer you their latest goods and services along with special discounts and selected products and services.

- You can choose to continue to receive information on special products and offers.
- You can choose not to have us share credit eligibility information within MBNA companies.
- You can choose not to have us share information with our partners.

- For a copy of MBNA's complete privacy policy, call us toll-free at 1-800-xxx-xxxx.
- To instruct us not to share credit eligibility information within MBNA, call 1-800-xxx-xxxx. We will ask you to verify your identity and your specific accounts or reference numbers. Please have your account, membership, or reference numbers (and for deposit accounts, your SSN or TIN) available when you call.
- To instruct us not to share information with our partners, call 1-800-xxx-xxxx. We will ask you to verify your identity and your specific accounts or reference numbers. Please have your account, membership, or reference numbers (and for deposit accounts, your SSN or TIN) available when you call.

THE HILL

JUNE 24, 2003

EDITORIAL

Preserve privacy

Under the terms of the Ninth Amendment, Americans should be able to enjoy what the late Supreme Court Justice William O. Douglas famously called a "right to be left alone." The federal criminal justice system should protect Americans as far as is feasible against identity theft.

Preserving these principles should be at the core of the privacy debate now simmering in Congress. And the executive branch needs to play a more active role in extending, expanding and standardizing federal laws that govern credit reports and other forms of consumer data sharing.

During the 2000 campaign, President Bush made several strong pro-privacy statements that cheered libertarian hearts. Post-Sept. 11 security makes some sacrifice of privacy necessary, but the White House must take minute care that every sacrifice is genuinely necessary. The two fundamental democratic rights, to security and to privacy, must be balanced not upended.

We commend those members of the financial services community who do not share client data with third-party marketers unless customers give them permission to do so. Congress should adopt similarly rigorous "opt-in" standards for it offers more genuine protection than an "opt-out," which allows sensitive information to roll down digital highways until and unless customers demand that it be blocked. Since most trade associations don't share these views, however, we recognize that stanching the flow won't be easy.

We support bipartisan efforts to pre-empt at the federal level a growing hodge-podge of state statutes that deal with credit reporting and financial privacy. This requires that the Fair Credit Reporting Act (FCRA) be extended and strengthened; the key provisions are due to expire at the year's end.

One good vehicle to accomplish such goals is H.R. 1766, the proposed National Uniform Privacy Standards Act, chiefly sponsored by Reps. Pat Tiberi (R-Ohio) and Ken Lucas (D-Ky.). Their legislation would keep FCRA alive and amend the Gramm-Leach-Bliley Act to prevent state and local governments sneaking through the patchwork of incompatible privacy rules.

FCRA mainly concerns financial information sharing among affiliates within financial services holding companies. Gramm-Leach-Bliley deals with how that data can be shared with third parties, such as auto dealers, furniture stores or small firms. These laws also ensure that consumers have ready credit.

We're pleased that officials of the Treasury Department and the Federal Trade Commission are coming to recognize that identity thieves take advantage of the states' varying standards which can make it difficult for credit card firms to discern unusual or fraudulent purchase patterns.

It's time for the administration to commit itself to extending FCRA and to championing privacy rights, consistent with responsible national security needs. Congress should do no less.

Questions from Congressman Ruben Hinojosa
For SAIC Tim Caddigan
Identity Theft Hearing
June 24, 2003

Question: In May 2003, CALPIRG Education Fund released the results of its interviews of with a sample of law enforcement officers from California and other cities with a high incidence of identity theft. Based upon the interviews, researchers concluded that: 1) identity theft is on the rise; 2) such crimes often remain unsolved; and 3) 85% of law enforcement officers believed that credit lenders should follow stricter requirements to ensure that credit is not granted to identity thieves. Are you aware of this study? Even if you are not familiar with this study, would you agree with the three findings in the report?

Answer: There is no question that identity theft is a growing crime that law enforcement agencies at all levels should be concerned about. The scope of identity theft is difficult to quantify. While the Federal Trade Commission receives thousands of identity theft reports and complaints each year, there are scores of other incidents that go unreported. Those of us in law enforcement are continuing to educate ourselves to work with private industry to provide information to the general public and form partnerships to combat identity crimes. Certainly it is in the best interests of both the industry and consumers for lenders to exercise due diligence when dealing with personal identification information.

Question: During the Senate Banking hearing on Identity Theft last week, Government experts felt that identity theft resulted from essentially four causes: people throwing out unshredded account information into the trash that is salvaged and used by others; people posting their personal information on the Internet for scam artists to use; co-workers or relatives directly stealing information and either selling or directly using that information; and computer hackers stealing information. What percentage of Identity Theft is not attributable to one of those four causes? Could it be that financial institutions' misuse of personal information is not the predominant cause of Identity Theft?

Answer: It is very difficult to say what percentage of identity theft is attributable to causes other than the four factors cited above. There are additional methods used by criminals to obtain personal and financial identifiers, such as the theft of U.S. mail, employees stealing customer information, and the use of electronic "skimming" devices. We recommend that any private business that obtains and/or stores personal or financial identifiers safeguard that information both from internal misuse as well as external theft.

COMMANDER MELLOTT

RESPONSE TO

QUESTIONS BY CONGRESSMAN RUBÉN HINOJOSA
HOUSE FINANCIAL SERVICES COMMITTEE
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS
"THE ROLE OF FCRA IN PREVENTING IDENTITY THEFT"
JUNE 24, 2003

1. Do you support the idea of providing consumers with a free credit report annually upon request?

   Yes Sir, I do.

2. Do you believe that would have prevented thieves from stealing your identity?

   While I doubt that a free credit report would have prevented the initial illegal use of my identity, since it would not have prevented a creditor from issuing credit on my Social Security Number without checking identity documents, it certainly would have notified me of this illegal use in a timely manner. Such notification would have certainly allowed me to implement protective measures and precluded subsequent use of my stolen identity.

3. I want to commend the FTC for its efforts to address ID theft, especially the release of its pamphlet in both English and Spanish entitled *Identity Theft: When Bad Things Happen to Your Good Name.* I placed a hyperlink to that publication on my website for my constituents to access if they believe they are victims of Identity Theft. There is an old saying that education is the key to success. In this instance, education is the key to fraud prevention. I applaud the FTC for the workshops it provides to the public to prevent ID Theft and to protect their privacy. To both witnesses, do you believe that the pamphlets that are provided by the FTC, the United States Postal Inspection Service and others is sufficient to address identity Theft or is legislation necessary?

   While education and the Identity Theft and Assumption Deterrence Act of 1998 are certainly important and essential, they are put two parts of a wider set of measures necessary to address this crime. In my personal opinion, additional legislation is necessary.

(continued next page)

COMMANDER MELLOTT RESPONSE TO QUESTIONS BY CONGRESSMAN RUBÉN HINOJOSA, HOUSE FINANCIAL SERVICES COMMITTEE, SUBCOMMITTEE ON FINANCIAL INSTITUTIONS, "THE ROLE OF FCRA IN PREVENTING IDENTITY THEFT," JUNE 24, 2003

If legislation is needed, what would you like incorporated into it?

(1) Any entity which is about to extend a loan, credit line or account, credit card, charge card, or utility service, must first: (a) positively verify identity documents before extending the loan, credit line or account, credit card, charge card, or utility service, and (b) check with all credit reporting agencies to determine if there is a fraud alert on file for any of the identity information provided on application documents. If there is a fraud alert, then it should be mandatory that the entity comply with the provisions of that alert. Failure to comply with these provisions shall result in direct monetary fines paid to the victim(s) any identity theft perpetrated via the loan, credit line or account, credit card, charge card, or utility service.

(2) Language similar to California Penal Code §530.8 which allows victims of identity theft to obtain copies of the unauthorized person's application or application information for, and a record of transactions or charges associated with, the loan, credit line or account, credit card, charge card, utility service, or account.

(3) Language that states that military law enforcement agencies (NCIS for example) shall record a report in all cases of identity theft perpetrated against active duty military members and against dependents of active duty military members. The military law enforcement agency shall provide a copy of the report to the military member or the dependant.

(4) Language that requires states to report statistics on the number of unsolved identity theft cases to the Federal Bureau of Investigation (FBI) and that the FBI shall publish those figures for public consumption.

(5) Language that mandates that victims of identity theft be notified no less than 48 hours in advance of any court appearance by the accused perpetrator of the crime. The victim shall be provided the case number and the day, time, and court in which the accused perpetrator will appear. The victim shall be afforded the opportunity to file a victim impact statement and to offer suggested conditions of probation that shall be read to the court before the any judgment or punishment is rendered.

(6) Language that requires to hold in abeyance any adverse credit information forwarded to a credit reporting agency on a deployed active duty military member if that member has filed a fraud alert with the agency. That hold shall remain in place for not less than six months after the member returns from overseas deployment.

(7) Should an individual provide a police report to a credit reporting agency, any fraud alert already on file or subsequently filed shall become permanent until removed by the individual via written and signed letter.

TESTIMONY OF THE

NATIONAL COMMUNITY REINVESTMENT COALITION (NCRC)

COMMITTEE ON FINANCIAL SERVICES

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

ON

"FIGHTING IDENTITY THEFT -- THE ROLE OF THE FCRA"

JUNE 24, 2003

SUBMITTED FOR THE RECORD BY

JOHN TAYLOR
PRESIDENT AND CEO

NATIONAL COMMUNITY REINVESTMENT COALITION
755 15TH STREET, NW
SUITE 540
WASHINGTON, DC 20005
(202) 628-8866

Good Morning Chairman Bachus, Ranking Member Sanders and Members of the Committee. My name is John Taylor, President and CEO of the National Community Reinvestment Coalition (NCRC). NCRC is a national trade association representing more than 600 community based organizations and who work daily to promote economic justice in America, and to increase fair and equal access to credit, capital and banking services to traditionally under-served populations in both urban and rural areas.

NCRC sincerely thanks you for the opportunity to testify before you today on the subject of identify theft. In particular, the focus of the testimony will provide NCRC's concern with the low and moderate-income consumers and their protection from the vulnerability of identity theft.

Low to moderate income families are identified as those who work the equivalent of a full-time job and earn between the minimum wage of $10,712 and approximately the median income in their area. According to a recent Census Bureau survey, the national median household income in 2001 was $42,228, down from $43,162 the previous year. In addition, we learned from a recent study by the Center for Housing Policy that the number of low-to moderate-income working families spending more than half their earnings on housing (much of it substandard housing) rose by over 67 percent ($4 million households) between 1997 and 2001. This study further revealed that part of the problem for low to moderate-income families was erosion of income, and the lack of affordable housing.

A great majority of the low to moderate-income population includes many elderly people. Many senior citizens are not privy to the consumer tips on identity theft and other scams targeting the elderly. Most of these families are struggling to meet their rent or mortgage payments, and usually have high medical bills and as well as high prescription costs. This is the population of people who are usually left out, the vulnerable and the unsophisticated.

A case in point deals with a recent hoax that targeted elderly African-Americans. Flyers were circulated in many Southern and Midwestern African-American communities, especially on car windshields in church parking lots, claiming that African-Americans born before 1928 could be eligible for slave reparations under a so-called "Slave Reparation Act". In addition, the hoax claimed that those born between 1917 and 1926 could apply for Social Security funds due them because of a "fix" in the Social Security System.

The claims were obviously false since no reparation law has ever been passed in the Congress. However, according to law enforcement officers, these claims were being alleged by skilled identity thieves who were asking people to reveal their name, address, phone number, birth-date and social security number in order to access their credit cards or open accounts under their names without their permission or knowledge.

A similar antic was proposed to many African-American farmers throughout the south. These farmers were asked to fill out an application and send in a check for $50.00 to participate in the settlement. Many of the farmers thought this was a legitimate proposal since the name of an attorney was listed on the application. Little did they know that the plaintiffs of the class action lawsuit had already been defined and had received a settlement

Finally, the following is a true story told by a woman named Dana is in fact unbelievable. Dana is a friend of a NCRC staff member:

"The following true story occurred over a year ago when a 38 year old woman, Dana Hunter Batts, owner of a daycare center at 7004____Street, closed her checking account, but failed to shred all of her old checks. Aware that all the checks were not shredded, she stood on her porch and watched the trashman pick up her garbage. Several weeks later Dana received notices that checks were bouncing. A total of $60,000 of returned checks showed up. One of the stores sent her a copy of the check, and she noticed that it had a false signature with a Maryland driver's license written on it. By this time least 200 stores were writing her for returned checks. Dana has been to court 3 times, and the police have come to her home to arrest her on several occasions. Dana went to the Department of Motor Vehicles and requested a criminal investigation. She discovered that a Maryland non-drivers license was issued to: Dana Hunter, 704____ Street. The thief actually sat for a picture, and put a different social security number and date of birth. Dana felt doomed, and felt she had " no where to turn, and nothing to do".

Dana wanted to post the picture of the thief, but was told that she could not do anything with the information she received because of the Privacy Act. She asked Motor Vehicle's staff how did they allow this to happen without checking ID, but to no avail.

Dana wrote to Chevy Chase Bank to let them know about the checks. She also wrote letters to about 200 stores, but she just got tired of keeping up. The police would come to arrest her so often that her reputation became ruined, and she had to close her daycare business and sell her home.

Dana was a college graduate and a nationally certified parametic. She initially had perfect credit. She requested her credit report and stated that now she cannot get a stick of gum. No one will accept her checks or allow her to get credit. She has to purchase everything in cash. She notified the credit bureaus, but they were of no assistance. Dana has had a bench warrant out for her arrest in almost every county in the metropolitan area.

Six months went by, and no checks were written. Dana thought the nightmare was over. After nine months, the thief started up again by purchasing new checks, but they were sent to a different address. Dana has notified the States Attorneys office, police officers in every jurisdiction and anyone else that will listen.

Now, Dana carries a photo of the thief with her at all times because she does not know when she will be stopped or arrested. She stated that she is tired, and cannot fight this system any longer. Dana has been on several job interviews, but feels that her poor credit rating was the reason that she was not hired. "

Over the course of a year, Dana has spent at least two to three hours every day working to resolve this issue. Dana is in school now since she cannot find a job. Every time the thief (who is still at large) writes a check and it bounces, the police come to her home to arrest her in the belief that she is the other woman. One store took her to court, and the company actually identified her as the person who wrote the check. Dana had to pull out the photo in order to contradict the storeowners. The emotional toil and the dollars spent by Dana are unmentionable. Dana feels that she has literally lost everything including her good name."

These three examples unfortunately are not isolated incidents. Low to moderate-income individuals often do not have the financial knowledge to realize that predators are targeting them. Working through NCRC members throughout the country, NCRC is tasked with providing financial education and training resources to low and moderate income communities throughout the United States in an effort to bring them into the financial mainstream. NCRC and its member organization recognize that financial education is at the very core of building communities and strengthening relations among community organizations, residents, small business and financial service providers.

NCRC's financial education program is unique and highly acclaimed with a three-tiered process involving trainers, resources and community-lender collaborations. This component builds basic money management skills, helps people to understand banking, finance and savings, and stresses the most important objective of maintaining good credit. We stress to our constituents that these are the tools an individual or family uses to save enough money to purchase a home or invest in a small business. NCRC also helps avoid being a victim of identity theft and consumer fraud. NCRC feels strongly that an understanding of capital is essential to financial growth for individuals and communities.

NCRC has recently incorporated into our financial education training program, the component of "protecting against fraud and identity theft", due to the numerous calls and requests received from NCRC member organizations, as well as from consumers who participate in our National Anti-Predatory Lending Consumer Rescue Fund. NCRC sees identity theft as one of the largest growing concerns to low and moderate income Americans. From the stories we have heard, most victims are usually unaware that a crime may have been perpetrated against them until they have practically lost their life's savings. Rebuilding and restoring their credit is daunting if even at all possible. As a result of the deceptive practices, many consumers have lost their homes forcing them into homeless shelters with a basic loss of consumer confidence in government and big business.

"Identity theft" is defined by the Federal Trade Commission (FTC) as: "Co-opting your name, Social Security number, credit card number, or some other piece of personal information for one's own use. " In short, the crime of identity theft occurs when someone appropriates your personal information without your knowledge to commit fraud or theft. As soon as the identity thief fakes another person's identity, it can have devastating effects on the victim.

Identity Theft can have devastating affects on its victims.
Examples include:

- Opening up a new credit card account using a name, address, date of birth, and Social Security number. A thief can access a consumer's public record that will enable them to discover places of employment, driver's license information and mother's maiden name.
- Credit card bills which fall delinquent due to the address and name (of the victim) not matching up.
- Establishing cellular phone service in your name, and similar to credit cards, bills are not paid.
- Opens a checking account, which enables bank accounts in your name and writes bad checks to be written.
- Takes out loans, purchases cars and real property in your name.
- Other categories include: employment - getting a job using the victim's name and identity, Social Security number, tax returns, residential leases, fraud, and miscellaneous government documents.

Due to the prevalence of identity theft, NCRC through its Financial Education and Consumer Rescue Fund to teach consumers the following regarding consumer fraud and identity theft:

Fraud and Identity Theft

Credit Cards:

- Tear up or shred all "pre-approved" credit card offers before throwing them away.

- Require that stores where one is seeking credit ensures that applications are treated as a secure document.

- Ask businesses how they store and dispose of credit card transaction slips. Ensure that proper safeguards are in place to treat these documents securely.

- Never give credit card numbers or other personal information over the phone unless you initiate the call. Even if the call is initiated, ensure that the called party is not using a cellular or other mobile phone.

- Carry only the needed credit cards when going on a trip to prevent credit cards from being lost or stolen.

- Sign credit cards in permanent ink as soon as they are received.

- Keep a list or photocopy of all credit accounts, along with expiration dates and phone numbers to call in case of theft. Keep this list in a secure spot in the home.

- When items are purchased with credit, always remember to take credit card receipts, and never throw them in wastebaskets or trash.

- Never have boxes of new checks delivered to your residence. Arrange to pick them up at the bank or credit union.

- Carefully examine each monthly credit card statement to ensure that every charge accurately matches credit card receipts.

- Do not write credit card numbers on checks.

- If a new credit card has been applied for and it does not arrive, contact the issuer.

- Avoid giving credit card numbers over the phone if in a public place. Even at work, others may overhear and use the information.

Social Security Number:

- Never carry documents containing your Social Security number. This includes Social Security cards as well as insurance cards.

- Never give your Social Security number to anyone by telephone, even if you make the call.

- Avoid having your Social Security number used for ID's at work. Request another one if possible. Also, avoid using your Social Security number as your drivers license number. Request that the Department of Motor Vehicles use an alternative number; most states will provide one.

Financial Transactions:

- Ask your bank or credit union to add additional security protection to your account.
- Shield your hand when entering your ATM password. Be aware of what is around you when approaching an ATM. Beware of persons looking over your shoulder with binoculars or a telephoto lens on a video camera.
- Memorize your ATM password and never write it down or keep it with you. Never write credit card numbers on you checks.
- Never pre-print or write your Drivers License or Social Security number on your checks.
- Never place bill payments in your home mailbox for pickup by postal carriers. Stolen checks can be altered and cashed by an imposter. Mail bills and other personal items at the post office.

Mail:

- Never sign up for unfamiliar contests or sweepstakes. Information provided by you could be sold and/or reproduced hundreds of times.
- Install a lockable mailbox at your home so thieves cannot easily take your mail.
- Remove your name from commercial marketing databases by writing to Direct Marketing Association's Mail Preference Service (P.O. Box 9008, Farmingdale, NY 11735) and Telephone Preference Service (P.O. Box 9015, Farmingdale, NY 11735).
- If your mail suddenly stops, check with the Post Office. Someone may have filed a change of address form.
- Stop credit bureaus from selling your name (header information). Call the toll-free telephone number used by all three credit bureaus and take advantage of their "opt-out" service. One number, (888) 5OPTOUT, or (888) 567-8688 reaches all three bureaus.
- Write to National Demographics and Lifestyles and ask to be deleted from its mailing list. National Demographics and Lifestyles, List Order Department 1621 18th Street, Suite 300 Denver, CO 80202. (800) 525-3533.

Credit Reports and other Documents:

- Shred all documents containing personal information before disposing of them. This includes utility bills, doctor's bills, bank statements, investment reports, and credit card receipts.

- Never post personal information on the Internet.

- Review your credit report annually. Access to free credit reports can be obtained on the website at: www.freeinstantcreditreports.com. This service can also assist with cleaning up your credit report.

- Add a fraud alert to your credit files that alerts all of the major credit bureau to inform credit givers to contact you for verification of any credit applications. Letters should contain your name, address, social security number, and spouse's name. Fraud alerts normally remain active for seven years.

Scams:

- Never respond to any scam by phone or email asking you to provide either credit card account information or your social security number.

- Sign in Rosters for colleges, agencies, programs (requesting name and social security numbers) – (state you will provide social security number in person)

- Email regarding a foreign government asking for your help in moving money from one account to another – Nigerian 419 Scam.

- Canadian/Netherlands Lottery – "You Have Won"

- "Free Credit Report" – Email scams

- "You have won a free gift" by phone or email about a free gift or prize. (Requesting credit card for shipping and handling) – Do not.

- Email chain letters/pyramid schemes. Example: (Bill Gates is testing anew email-tracking program and wants your help. If you forward email to your friends, Microsoft will pay you $_ for each person that receives it.)

- "Find out everything on anyone" – Email trying to solicit dollars in order to buy a CD or program that you can use to find out personal information on another person.

- Questionnaires – Email holiday card requesting birth date and social security number from "old friend" from a chat room.

- Account Verification Scams – Individuals who have purchased domain names similar to those of legitimate companies. The latest is Discover Card, e-gold.com, ebay-verification.net and change-ebay.com. Companies victimized by the scam are AOL, MSN, Earthlink, E-Bay, PayPal, Discover Card, Bank of America, Providian and Wells Fargo.

- "Help Wanted" ad on Internet – Do not put Social Security numbers on resumes.

- Job Advertisement Scams - Internet Job Web-sites (i.e. Monster.com) and Newspaper Want Ads. (No applicant should respond to a HR person especially giving out a Social Security Number)

- In-Store security scams (requesting that a customer assist in catching a bad employee by asking for personal information or pre-filled application that the customer gave to the employee).

- Telephone scams– Charities asking for donations or calls asking to be included on a "do not call list" requesting Social Security numbers.

- Others include - IRS scams, PayPal Scam, Order or Gift Confirmation, Get out of Debt Scams, Social Security Services Scams, and numerous others.

NCRC and other consumer advocacy groups have serious concerns about the reauthorization of these FCRA provisions and its impact on the exercise of states rights and strong and adequate consumer protection of citizens.

Outline of NCRC's Recommendations:

- NCRC believes strongly that in the event that a crime of identity theft is committed, the consumer should have an expedient right of redress with law enforcement as well as the regulated cooperation of credit reporting agencies and their furnishers. NCRC believes that perpetrators of identity theft scams must face swift and severe justice.

- Federal pre-emptions should be allowed to expire as intended by FCRA unless Congress enacts uniform federal legislation providing strong consumer protections and criminal sanctions for identity theft.

- If reauthorization of FCRA occurs with federal standards and pre-emptions. NCRC feels strongly that states with stronger consumer protection laws like California (particularly with regard to identify theft), should not be compelled to nullify their laws. Exceptions for such states should be designated in the legislation.

- NCRC strongly believes that reasonable steps should be made to strengthen the obligations of furnishers to report timely and accurate information. Primarily, efforts should be made by the furnishers of information, as well as the credit reporting agencies to complete any disputes regarding a consumer's credit record with an

investigative period or re-investigative period of less than 30 days. Further, if the investigation or re-investigation extends longer than the designated period, notification should be made to the consumer in writing with an identifiable timeframe for completing the investigation included in the notice. Currently, the FCRA establishes 30 days for the initial investigation of a dispute and allows for a 15 day extension. NCRC believes that in this era of computerization, these time periods could be shortened to 20 and 10 days, respectively. Consumers should not have to wait a month and a half for resolution of complaints; one month ought to be sufficient.

- NCRC further believes that additional steps should be taken to notify consumers within 10 days of receipt of any derogatory or negative information disseminated by the furnisher of information or the credit reporting agency. The letter should spell out specifically the nature of the negative or derogatory information rather than using vague terminology. In addition, the re-authorized law should designate which entity or both should be responsible for notifying the consumer.

In Addition, NCRC Recommends the Following:

- Congress must significantly expand the role of the FTC in prosecuting and resolving identify theft cases. The Identity Theft Assumption and Deterrence Act of 1998 requires the FTC to establish a centralized database of identify theft cases and to coordinate efforts with federal and state enforcement agencies. The case study of Dana described in the beginning of our testimony demonstrates that the existing system is failing to protect thousands of citizens like "Dana". No enforcement agency has ended this identity theft scam, which is ruining Dana's life. In Dana's example, multiple state and local police departments have failed to close the case. The FTC must be empowered to act as an enforcement agency, prosecuting cases and assigning priority to cases that have plagued consumers for years and in multiple jurisdictions as in Dana's case. Congress must provide appropriations to the FTC so that the agency can adequately staff an office designated to resolve identify theft cases.

- Credit Reporting Agencies should be compelled under FCRA to redesign their credit reports so that they are consumer or user friendly and understandable to the average lay person. The instructions should be simplified and outline the mechanics of what the credit report/score entails. The same should be implemented for "opt-out" procedures in privacy notices.

- The credit industry should implement the practice of verifying at least three pieces of information, such as the name, address, date of birth, Social Security number, drivers license number and place of employment, with information on the existing credit report. This is extremely important when the consumer is requesting instant credit. If the consumer is applying in person, however, the credit grantor should always be required to inspect a photo ID.

- If credit is offered via a mailed application (often referred to as pre-approved offers), measures should be taken to ensure that the credit grantor uses the consumer's address exactly as it appears on the original solicitation, not a different address, which could easily be the work of an identity theft. In addition, if the card issuer receives a change of address notification, it must also send a confirmation notice to the old address it has on file.

- Consumers should be provided with at least one free copy of the credit report annually from each credit bureau. (Maryland, Colorado, Georgia, Massachusetts, New Jersey, and Vermont already have passed these laws.) If consumers checked their credit reports regularly, identity theft would be detected earlier, and the overall impact minimized.

- Further, consumers should be able to have easy access to their credit files through a secured system with each credit bureau at their convenience even if there is a cost factor.

- Allow consumers to have a "freeze" on their credit reports preventing their reports from being furnished without specific authorization.

NCRC Supports Legislation:

NCRC supports the following legislation regarding identity theft in a comprehensive nature:

1. NCRC supports Congressman Bernie Sanders (I-VT) bill, H.R. 2546, the Free Credit Report Act of 2003, which requires consumer reporting agencies to provide any consumer with a free credit report annually upon the request of the consumer.

2. NCRC supports bi-partisan legislation, HR 3368, introduced by Rep. Schakowsky and Rep. Bachus to close a loophole, making it harder for identify theft victims to sue credit bureaus. In November of 2001, the Supreme Court ruled that FCRA's statute of limitations applies to the two year time period after fraud has been committed. HR 3368 would stipulate that two year time period would not begin until the borrower has discovered the fraud.

3. Senator Maria Cantwell's (D-WA) "Identity Theft Victims Assistance Act of 2002" which establishes a nation-wide process for victims of identity theft to obtain business records related to an identity theft, to facilitate the victim's correction of false records and assist law enforcement in obtaining evidence to apprehend the identity thieves. This legislation also clarifies that for victims of identity theft, the statute of limitations for the Fair Credit Reporting Act will be five years, rather than the current two, addressing the Supreme Court's decision in *TRW v. Andrews*. This bill requires consumer credit reporting agencies to block reporting of bad credit arising from identity theft. This bill expands the role of the federal Coordinating Committee on False Identification beyond the current mandate to review federal enforcement of

identity theft law and also examine state and local enforcement and terrorist activity with regard to identity theft.

4. NCRC also supports Senator Diane Feinstein (D-Ca) who introduced legislation in the 107th Congress enhancing the penalties for any individual who steals an identity and uses that false identity to commit one of a number of serious federal offenses including immigration offenses, firearms offenses, and false citizenship crimes.

5. Senator Feinstein also introduced legislation prohibited anyone from selling or displaying a Social Security number to the general public without the Social Security number holder's consent. This provides tools for identity theft victims to restore their identity.

6. NCRC supports the legislation of Congressman Jerry Keczka (D-Wis) that would prohibit businesses from obtaining or distributing a person's social security number without the person's written consent. The bill would also stop credit bureaus from selling "credit headers" – the top portion of credit reports – without consent. The credit headers lists a consumer's name, address and telephone number (including unlisted ones), mother's maiden name, date of birth and Social Security number which earn credit bureaus millions of dollars annually.

7. NCRC supports two bills offering consumer control over their personal financial information. H.R. 3320, introduced by Congressmen Ed Markey (D-Ma) and Joe Barton (R-TX) and S 1903, introduced by Senators Richard Shelby (R-AL) and Richard H. Bryan (D-NV). Both bills require banks to obtain the consent of consumers before selling or sharing information (opt-in). If consumers do not respond, the banks would not be free to sell or share their information.

8. NCRC supports H.R. 3053, Identity Theft Prevention Act of 2001, introduced by Congresswoman Darlene Hooley. The bill amends the Truth in Lending Act to prescribe procedural guidelines under which a credit card issuer shall confirm changes of address. It also amends the Fair Credit Reporting Act to prescribe procedural guidelines under which a consumer reporting agency shall: (1) notify the requester of a discrepancy in the address in the consumer file; (2) include a fraud alert in the file of a requesting consumer; and (3) make free annual disclosures upon the consumer request. It also confers enforcement jurisdiction upon the Federal Trade Commission.

9. NCRC supports California Law SB 168 (Debra Bowen) "Identity Theft Prevention" which prevents identity theft by taking Social Security numbers out of the public's view and the easy reach of criminals by making it illegal for businesses to do any of the following: (1) Post or display social security numbers; (2) Print social security numbers on identification cards; (3) Require a person to transmit a social security number over the internet unless the connection is secure or the social security number is encrypted; (4) Require a person to use a social security number to log onto an internet web site unless used in combination with a password or other authentication

device; and (5) Print a social security number on any materials mailed to a customer unless it's required by law, or the document is a form or application.

The bill also prevents identity theft by giving people the right to "freeze" access to their credit reports. By placing a freeze on a credit report, an identity thief will not be able to get new loans or credit in the victim's name since lenders, retailers, utilities and other businesses need access to a credit report to review and approve new credit loans, and services. At the same time, the bill makes sure people who have frozen their credit reports can still get new loans and credit through access to a PIN based system set up through the credit reporting agencies.

10. NCRC applauds SB 1365, authored by Senator Kevin Murray (D-Culver City, CA), This bill would allow victims of identity theft to prohibit companies with which they do business from sharing marketing information about them with affiliates and third parties. If a company disclosed customer information to a felon, it could be held liable for a penalty of $5,000 per disclosure.

CLOSING:

NCRC shares many of the concerns of other consumer advocates with regard to revamping the Federal Credit Reporting Act. We also share the view that for too long Credit Reporting Agencies and furnishers of information have operated with loose guidelines and little accountability to the consumer.

As testimony after testimony has revealed, more than a thousand consumers a day across all socio-economic demographics are being hurt financially, professionally and emotionally from perpetrators who can simply go on the internet to obtain personal information and perpetuate fraud and identity theft. As a result, these victims are charged to get their life back in order by using, according to GAO study, an average of 175 man-hours and an average out-of- pocket expense of $1400. The emotional toil spent to recoup their identity and restore their credit and lifestyle back to status quo is beyond comprehension.

Many low to moderate-income families never have this luxury for lack of resources and knowledge. We are in an information age where access to intelligence, personal information and sensitive data are too easily accessible. Mr. Chair, Americans have a right to their privacy, and the Credit Reporting Agencies are not holding up to their end of the bargain. These types of crimes are foreseeable and inevitable, and victim assistance is critical. Little effort has been made on behalf of consumers to correct these wrongs.

NCRC supports strengthened federal, state and local laws which hold perpetrators strictly accountable. The consumer reporting agencies must be reformed to protect consumers through quick resolution of erroneous information and easy access to their credit files. Finally, NCRC looks forward to working with you and the other Members of the Committee on revamping the FCRA.

O